# MACsec
## Critical point-to-point protection

Xiphera's Security Protocols family offers data protection for the most demanding security levels on critical communication links. The comprehensive MACsec IP (Intellectual Property) core portfolio protects both the confidentiality and integrity of transmitted data on a point-to-point Ethernet link. The underlying cryptographic engines in the MACsec solutions are based on Xiphera's own AES-GCM IP cores.

### Standard compliance

- MACsec protocol secures the Data Link layer in the widely accepted OSI (Open System Interconnection) model
- Xiphera's MACsec IP cores are fully compliant with the industry-wide established standard IEEE Std. 802.1AE-2018
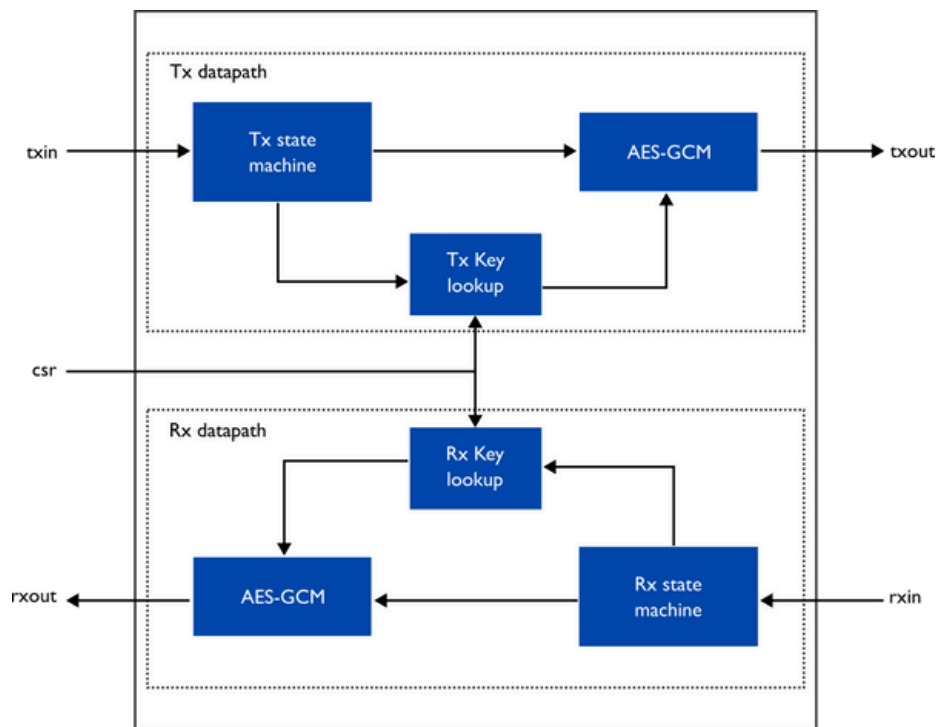
### Optimised performance

- Xiphera's various MACsec variants offer optimal solutions for different needs, depending on individual resource and performance requirements of the customer
- The extreme-speed MACsec IP core pushes performance to hundreds of Gbps

### Special features

- All Xiphera's MACsec IP cores support VLAN as cleartext
- The number of secure connections per MACsec port can be set by the user

XIPHERA

# High-level block diagram of 100G MACsec AES256-GCM IP core



## About Xiphera

Xiphera designs and implements proven cryptographic security for embedded systems. Our strong cryptographic expertise and extensive experience in digital system design enable us to help our customers to protect their most valuable assets. We offer secure and highly optimised cryptographic Intellectual Property (IP) cores, designed directly for FPGAs and ASICs without software components. Our broad, fully in-house designed, and up-to-date portfolio enables cost-effective development projects with fast time-to-market – providing peace of mind in a dangerous world.