BittWare
a molex company

Partner IP

XIPHERA
PEACE OF MIND IN A DANGEROUS WORLD

IPsec

Extreme Speed IPsec IP Core

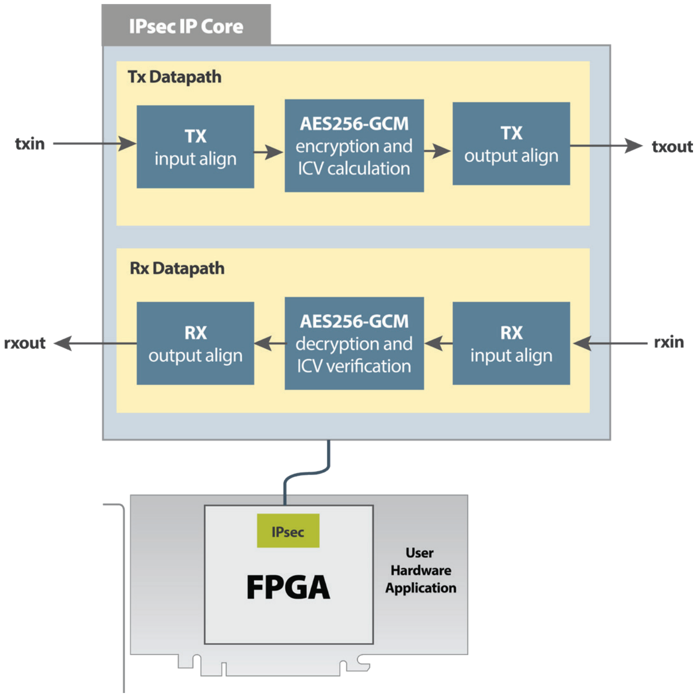
IPsec (Internet Protocol Security) is a widely accepted and adopted security protocol, ensuring secure communication over the Internet. Xiphera's IPsec core implements ESP (Encapsulating Security Payload) frame processing in the IPsec protocol using Xiphera's own AES256-GCM. The IPsec protocol secures the communication traffic on Layer 3 of the OSI model by assuring that a received frame has been sent by a transmitting station that claimed to send it, and by encrypting the contents.

Xiphera's scalable extreme-speed IPsec IP core (XIP7013E) is best suited for traffic on links from 10 Gb/s to 200 Gb/s links with high-end FPGAs. The IP core has been designed for easy integration for FPGAs in a vendor-agnostic design methodology.

ESP frame processing

up to 200 Gb/s throughput

Compliant with **IPsec protocol**



Features

Performance:

- The extreme-speed IPsec achieves a throughput in the 200 Gb/s range
- The IP core does not require any extra interpacket gap cycles even when it processes short packets

Standard Compliance:

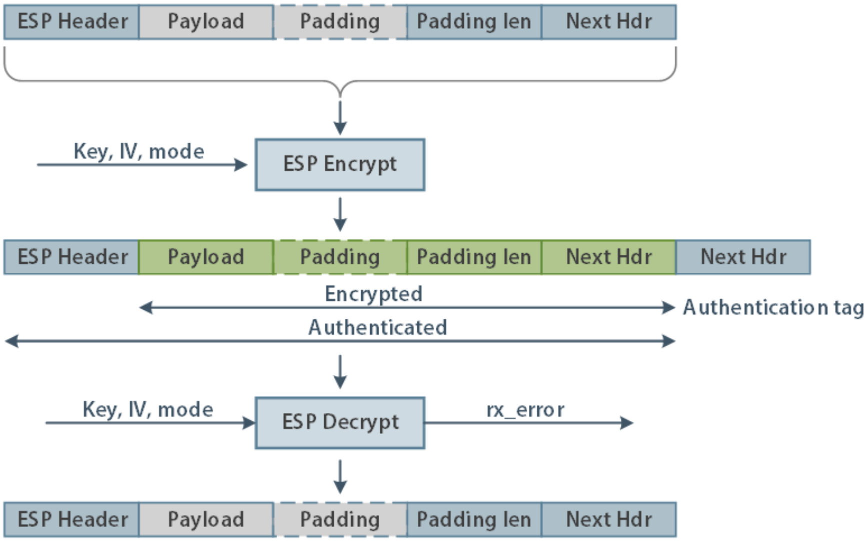
- The scalable IPsec is compliant with RFC4303
- The cipher suite (AES256- GCM) is fully compliant with the Advanced Encryption Algorithm (AES) standard, as well as with the Galois Counter Mode (GCM) standard

Easy Interfacing:

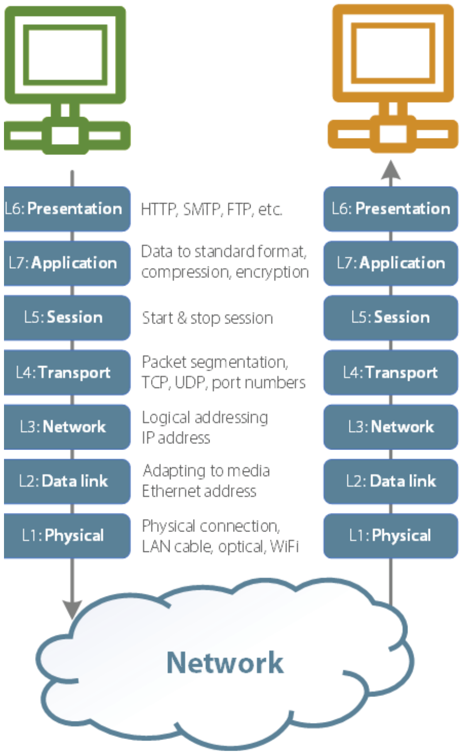
- The extreme-speed IPsec uses a streaming interface for payload data and side-channel signalling for the required ESP frame parameters

Functionality

The XIP7013E IP encrypts and authenticates IPsec ESP (Encapsulating Security Payload) packets in the Transmit (Tx) direction and decrypts and validates the authenticity of IPsec ESP packets in the receive (Rx) direction. The ESP packet processing can be used in five different modes allowing either payload authentication, encryption with or without optional IV (Initialisation Vector), or bypassing the payload as it is.



IPsec High Level Functionality



OSI Network Model

FPGA Resources and Performance

The table below presents the FPGA resource requirements on the Altera Agilex® 7:

FPGA Family	Resources	fmax	Databus Width	Max Throughput
Altera Agilex® 7	86000 ALMs, 4 M20K	463.39 MHz	512-bit	220+ Gb/s
	50000 ALMs, 4 M20K	486.38 MHz	256-bit	124+ Gb/s

Altera target device: AGFA006R16211V, Quartus version 23.2

Deliverables

XIP7013E can be shipped in several formats, including netlist, source code, or encrypted source code. A comprehensive SystemVerilog testbench and a detailed datasheet are included.

Compatible FPGA Cards

- IA-840F
- IA-420F

Looking for a different card? Ask us about additional compatible card options. We can port from Agilex 7 F-Series to I-Series, M-Series, and AMD UltraScale+.

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

v0 | last revised 2024.03.22

BittWare
a molex company