



PEACE OF MIND IN A DANGEROUS WORLD

# XIP7213E: IPSEC AES-256-GCM

## Extreme-Speed IPsec

Product Brief  
ver. 0.9  
2025-11-26

sales@xiphera.com

---

### Introduction

XIP7213E implements the Internet Protocol Security (IPsec) as standardised in RFC4303 and RFC4305. The IPsec protocol defines a security infrastructure for Layer 3 (as per the OSI model) traffic by assuring that a received packet has been sent by the transmitting station that claimed to send it. Furthermore, the traffic between stations is both encrypted to provide data confidentiality and authenticated to provide data integrity.

XIP7213E uses Advanced Encryption Standard [1] (AES) with 128/256-bit key in Galois Counter Mode (GCM) [2] to protect data confidentiality, data integrity and data origin authentication. The cipher suite is denoted as GCM-AES(-XPN)-128/192/256 and with 8/12/16 byte authentication tag. Both 32 or 64-bit sequence numbering is supported. XIP7213E uses Xiphera's extreme-speed AES-GCM IP core XIP1113E as the underlying building block for Authenticated Encryption and Associated Data (AEAD).

Secure Association Database (SAD) lookup for frames is performed by XIP7213E independently and Secure Association (SA) management (IKEv2 / RFC4306) is offloaded to a CPU/MCU via separate secure interface.

XIP7213E has been designed for easy integration with FPGA- and ASIC-based designs in a vendor-agnostic design methodology, and the functionality does not rely on any vendor or process-specific features

### Key Features

- **Performance:** The extreme-speed XIP7213E achieves a throughput exceeding 100 Gbps range in modern high-end FPGAs and ASIC process nodes. Notably XIP7213E does not require any extra idle cycles, even when it processes short packets.
- **Standard Compliance:** XIP7213E is compliant with the IPsec protocol as standardised in RFC4303 [4] / RFC4306[3]. The cipher suite (GCM-AES-128/192/256) is fully compliant with

the Advanced Encryption Algorithm (AES) standard [1], as well as with the Galois Counter Mode (GCM) standard [2].

- **Fully standalone IPsec** engine, requiring no external CPU or software intervention for packet encryption, authentication, or flow management, offers performance, security, low power consumption and ease of validation.
- **Flexible key management** interface with IKEv2 support, enabling smooth integration with existing security frameworks and automated key lifecycle handling.
- **CAVP validated:** The underlying cryptographic algorithm implementations in the XIP7213E have received [5] Cryptographic Algorithm Validation Program (CAVP) [6] validation. <sup>1</sup>

## Functionality

The functionality of XIP7213E is divided into the transmit (Tx) and receive (Rx) datapaths, which operate independently of each other. The underlying cipher suite AES-GCM is consequently instantiated for both the Rx and Tx datapaths.

IPsec operation is based on the concepts of unidirectional Security Associations (SA) within each channel. Each SA uses its own Secure Association Key (SAK); establishing and managing keys is not part of the IPsec standard.

The high-level functionality of Tx datapath includes parameter lookup based on source and destination IPs, ports and protocol. Based on these parameters the IP constructs the TX output frame with encrypted and authenticated ESP frame. TX path also has an option to insert IKEv2 frames from internal buffer, which can be updated by CPU interface.

The high-level functionality of RX datapath includes IPsec frame detection, either based on ESP protocol type or UDP encapsulated frames, with port numbers 500 or 4500. IKEv2 frames are recognised based on SPI information and state of IKEv2 process.

XIP7213E also supports the bypass mode, where an incoming packet passes through the XIP7213E unaltered.

---

<sup>1</sup>The certifications are valid for a certain version of the XIP7213E IP core.

## Block Diagram

The internal high-level block diagram of XIP7213E is depicted in Figure 1.

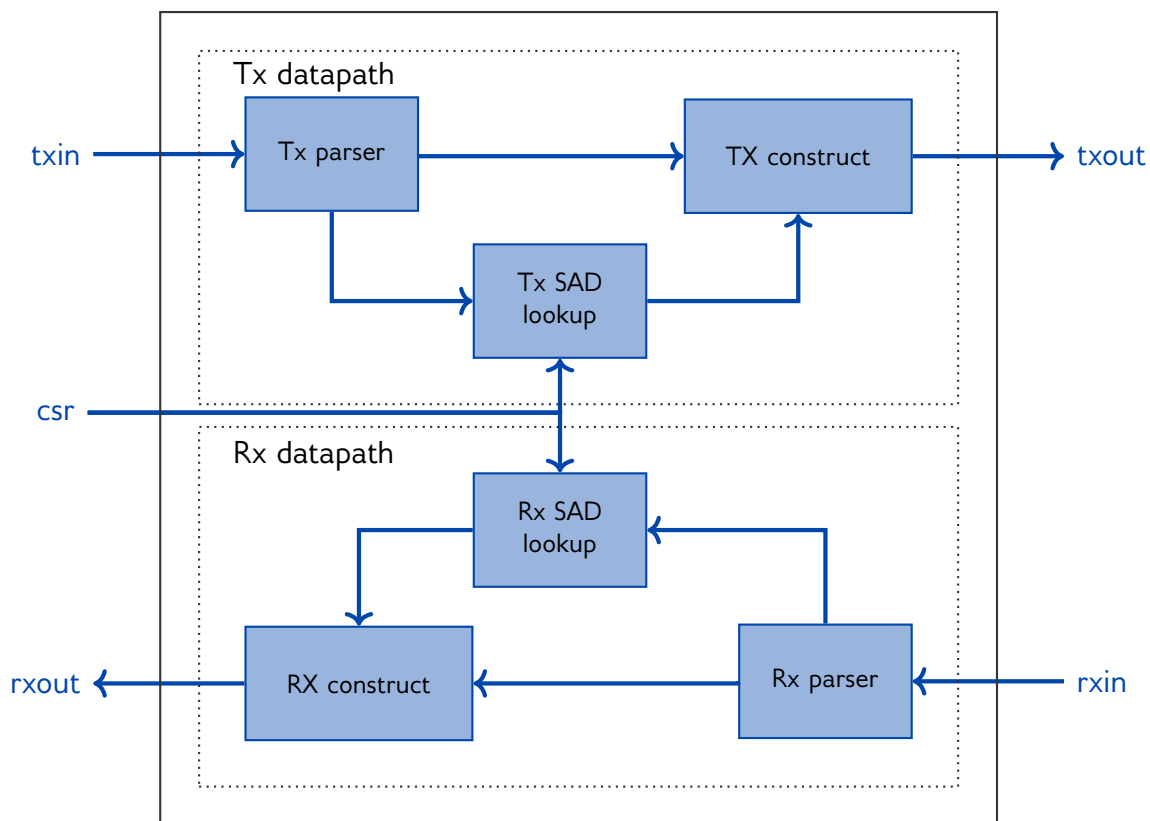


Figure 1: Internal high-level block diagram of XIP7213E.

## Interfaces

The external interfaces of XIP7213E are depicted in Figure 2, and can be grouped into five logical groups:

- One Control and Status Register interface, I/O signal names beginning with `csr`
- Two Transmit interfaces, I/O signal names beginning with `txin` and `txout`
- Two Receive interfaces, I/O signal names beginning with `rxin` and `rxout`

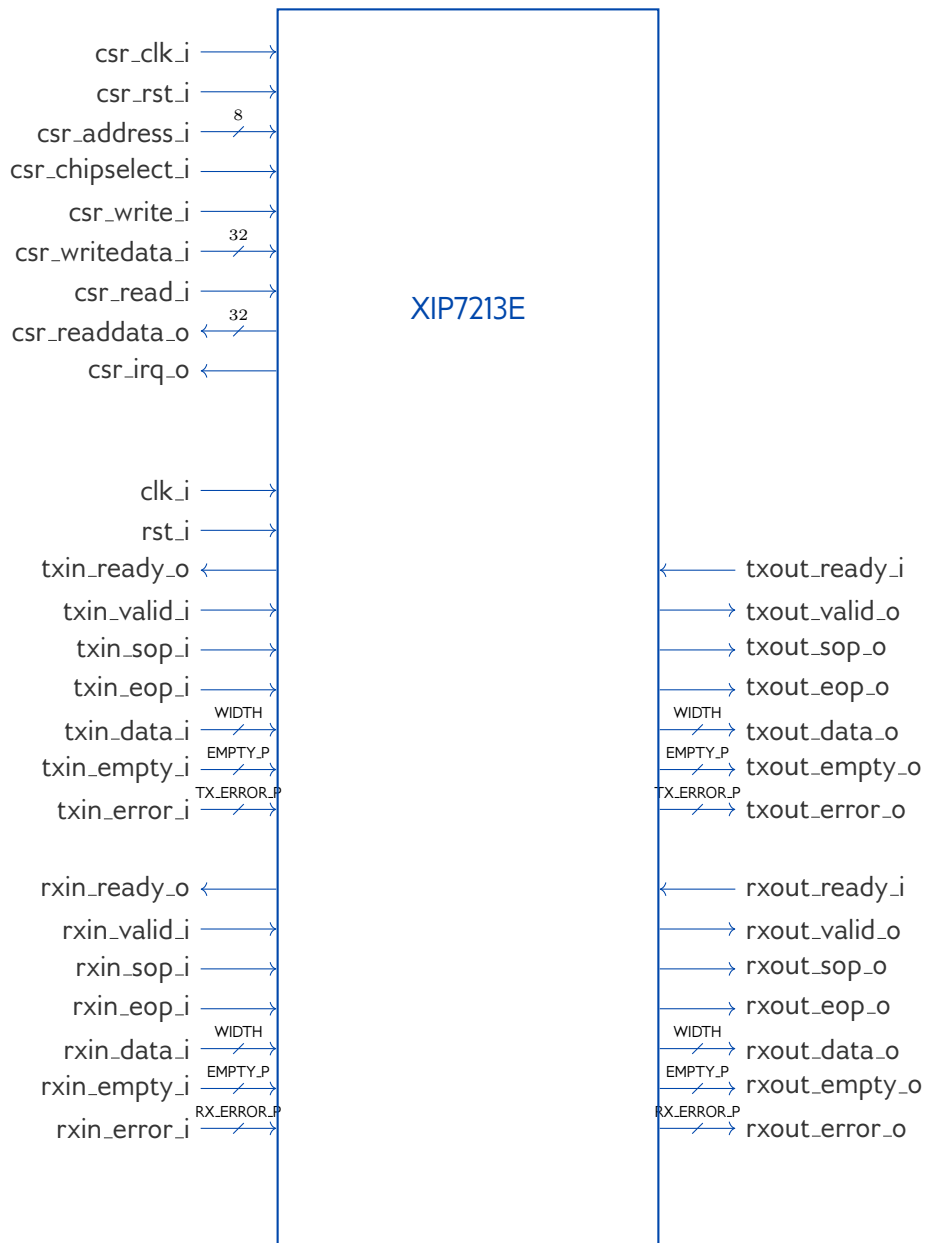


Figure 2: External interfaces of XIP7213E with RX and TX interfaces.

## Example Use Cases

The primary application of XIP7213E is to provide confidentiality and integrity of data as well as header authentication for Layer 3 connections. Consequently, XIP7213E is typically connected via an EMAC IP core to an external Ethernet link<sup>2</sup>, and the CSR (Control and Status Register) interface is connected to a processor<sup>3</sup>. An example use case is presented in Figure 3.

<sup>2</sup>Representative Ethernet speed is 100 Gbps. Higher speeds can be supported by instantiating multiple XIP7213E instances in parallel.

<sup>3</sup>The processor can also be an FPGA-based soft processor.

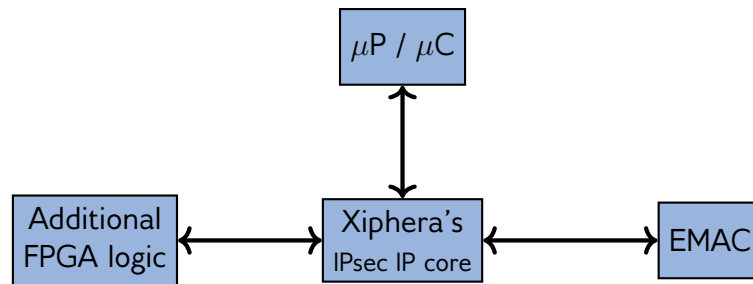


Figure 3: Example use case for XIP7213E.

## Ordering and Deliverables

Please contact [sales@xiphera.com](mailto:sales@xiphera.com) for pricing and your preferred delivery method. XIP7213E can be shipped in a number of formats, including netlist, encrypted, obfuscated or plain text source code. Additionally, synthesis scripts, a comprehensive testbench, and a detailed datasheet including an integration guide are included.

## Export Control

XIP7213E protects data confidentiality and is a dual-use product as defined in the Wassenaar Arrangement. Consequently, the export of XIP7213E is controlled by Council Regulation (EC) No 2021/821 and its subsequent changes.

XIP7213E can be immediately shipped to all European Union member states, Australia, Canada, Japan, New Zealand, Norway, Switzerland, United Kingdom, and the United States.

Export to other countries requires authorization from The Ministry for Foreign Affairs of Finland, and typical processing time for an export authorization is few weeks.

## About Xiphera

Xiphera specializes in secure and efficient implementations of standardised cryptographic algorithms on Field Programmable Gate Arrays (FPGAs) and Application Specific Integrated Circuits (ASICs). Our fully in-house designed product portfolio includes individual cryptographic Intellectual Property (IP) cores, as well as comprehensive security solutions built from a combination of individual IP cores.

Xiphera is a Finnish company operating under the laws of the Republic of Finland, and is fully owned by Finnish citizens and institutional investors.

## Contact

Xiphera Oy  
Tekniikantie 12  
FIN-02150 Espoo  
Finland  
[sales@xiphera.com](mailto:sales@xiphera.com)  
+358 20 730 5252

---

## References

- [1] Specification for the Advanced Encryption Standard (AES). Federal Information Processing Standards Publication 197, 2001.
- [2] 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.
- [3] Charlie Kaufman. Internet Key Exchange (IKEv2) Protocol. RFC 4306, December 2005.
- [4] Stephen Kent. IP Encapsulating Security Payload (ESP). RFC 4303, December 2005.
- [5] National Institute of Standards and Technology. CAVP Algorithm Validation Listings — Xiphera Ltd. Online database entry, 2025. <https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program/validation-search?searchMode=implementation&vendor=Xiphera+Ltd>.
- [6] National Institute of Standards and Technology. Cryptographic algorithm validation program (cavp). Technical report, U.S. Department of Commerce, National Institute of Standards and Technology, 2025. Accessed 2025-11-26.