XIPHERA

PEACE OF MIND IN A DANGEROUS WORLD

XIP7131C: TLS 1.3 AES256-GCM

Compact IP Core for TLS 1.3 Secure Communication

Product Brief

ver. 1.3.3 2026-08-04

sales@xiphera.com

Introduction

XIP7131C is a compact IP core implementing the TLS (Transport Layer Security) 1.3 protocol as defined in RFC 8446 [9]. TLS is the cryptographic protocol used to build a secure connection between a client and a server over the Internet, and a hardware-based implementation such as XIP7131C enables a high level of security for mission-critical industries by ensuring that security-critical operations are entirely self-reliant on hardware, eliminating the need for a TLS software stack in the surrounding system.

XIP7131C implements a selected TLS 1.3 cipher suite built around AES256-GCM [1, 5] authenticated encryption for the record layer, ECDH [2] key exchange and ECDSA [4] authentication for the handshake, and HKDF [6] key derivation based on HMAC and SHA-2 [3]. ChaCha20-Poly1305 [8] authenticated encryption is also available as an alternative to AES256-GCM upon request. An internal TRNG (True Random Number Generator) supplies the entropy required for key and nonce generation, and all generated and derived key material is held in dedicated on-chip key storage so that it never needs to leave the hardware boundary.

Despite this extensive feature set, XIP7131C maintains a compact footprint. The implementation is target architecture agnostic, portable and fully compliant with all ASIC process nodes and FPGA platforms without any need for hard macros, vendor specific functions or internal memories.

If required, post-quantum protection of the TLS 1.3 handshake [10] can be added to XIP7131C using Xiphera's xQlave® family of Post-Quantum Cryptography IP cores.

Key Features

- **Compliant:** XIP7131C implements the TLS 1.3 protocol as defined in RFC 8446 [9], using a selected cipher suite built entirely from standardised cryptographic algorithms.
- **Client and server:** XIP7131C can be delivered in a client or in a server configuration, with client authentication supported in both roles.

- **Compact:** XIP7131C has minimal resource requirements, using approximately 20 kLUTs on FPGAs, providing an excellent fit for high-volume FPGA and ASIC applications while sustaining over 1 Gbps of bulk (client-side) traffic throughput.
- **1G/2.5G full-duplex:** XIP7131C targets 1G and 2.5G full-duplex networking systems, protecting the transmit and receive directions simultaneously and with low latency.
- **Powered by AES256-GCM:** XIP7131C uses AES256-GCM [1, 5] authenticated encryption to protect the TLS 1.3 record layer, providing a high level of security for bulk data.
- **ChaCha20-Poly1305 available:** As an alternative to AES256-GCM, XIP7131C can be configured with ChaCha20-Poly1305 [8] authenticated encryption upon request.
- **Scalable to higher line rates:** the balanced AES256-GCM core can be exchanged for an Extreme Speed variant upon request, targeting line rates from 10G up to 400G.
- **Hundreds of sessions:** XIP7131C holds the key material and protocol state for hundreds of simultaneous TLS 1.3 sessions on-chip.
- **Transparent to the host:** XIP7131C consumes plaintext and emits the corresponding TLS 1.3 records in the transmit direction, and reverses the process in the receive direction, leaving the record layer invisible to the host. Traffic other than TLS 1.3 records is bypassed and passed through unmodified, so protected and unprotected flows can share a single datapath.
- **Hardware-based key management:** XIP7131C generates, derives and stores all session key material on-chip, including an internal TRNG for entropy generation, so that cryptographic operations are performed directly in hardware for both security and performance.
- **Easy system integration:** XIP7131C is controlled through a single AXI4-Lite interface and exchanges payload data over standard AXI4-Stream interfaces, and is delivered with a comprehensive datasheet and integration guide to simplify integration into the customer's system.
- **Vendor agnostic:** XIP7131C is target architecture agnostic, portable and fully compliant with all ASIC process nodes and FPGA platforms without any need for hard macros, vendor specific functions or internal memories.

Functionality

XIP7131C performs the complete TLS 1.3 protocol in hardware, covering both the handshake and the record protocol, and sits between a secure side, carrying plaintext application data, and an insecure side, carrying the corresponding TLS 1.3 protected traffic exchanged with the untrusted network. XIP7131C can be delivered in a client or in a server configuration, and holds the key material and protocol state for hundreds of simultaneous TLS 1.3 sessions.

During the handshake, XIP7131C uses ECDH to establish a shared secret with the peer and ECDSA to authenticate the connection, including client authentication where the deployment requires it, and derives the traffic keys required for the session using HKDF based on HMAC and SHA-2. All generated and derived key material is stored in dedicated on-chip key storage and never needs to be exposed outside XIP7131C.

Once the handshake has completed, XIP7131C uses the derived session keys to protect the TLS 1.3 record layer with AES256-GCM (or, upon request, ChaCha20-Poly1305) authenticated encryption: outgoing plaintext received on the secure side is encrypted and authenticated into ciphertext

delivered on the insecure side, while incoming ciphertext received on the insecure side is decrypted and its authenticity validated before the resulting plaintext is delivered on the secure side. The plaintext consumed on the secure side and the TLS 1.3 records produced on the insecure side are both carried as ordinary TCP payload, so the record layer remains invisible to the host and to the TCP/IP stack transporting the records. Traffic that does not belong to a protected session is bypassed and passed through XIP7131C unmodified, allowing protected and unprotected flows to share a single datapath. For line rates beyond the 1G and 2.5G full-duplex operation of the balanced configuration, the AES256-GCM core can be exchanged for an Extreme Speed variant upon request, scaling XIP7131C to line rates from 10G up to 400G.

XIP7131C is controlled and configured through an AXI4-Lite interface, while plaintext and ciphertext are exchanged over separate AXI4-Stream interfaces for the transmit and receive directions. The handshake and the record protocol are sequenced autonomously by the internal control subsystem of XIP7131C, so that the surrounding system issues only high-level commands, such as opening a connection or requesting a key update, and reads back the corresponding status; no TLS protocol implementation is required in the surrounding system. An internal TRNG (True Random Number Generator) provides the entropy required throughout the protocol for key and nonce generation.

Block Diagram

The internal high-level block diagram of XIP7131C is depicted in Figure 1.

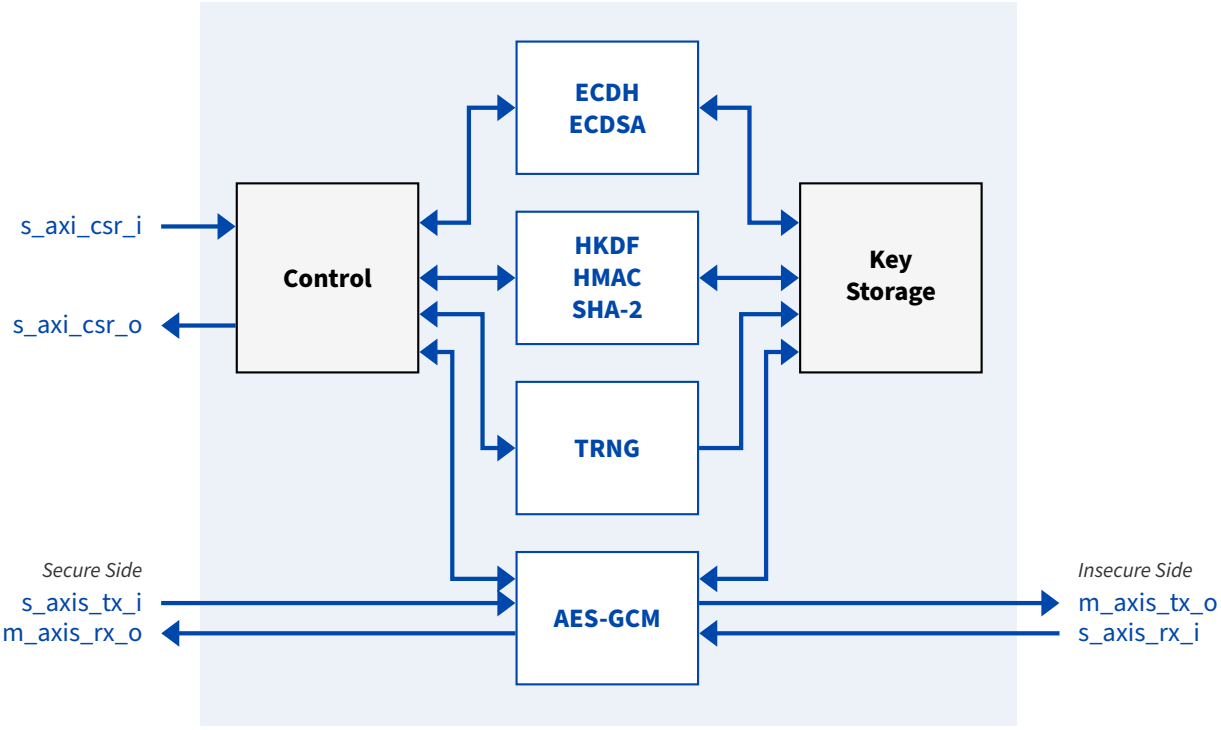

Figure 1: Internal high-level block diagram of XIP7131C

XIP7131C integrates Xiphera's individually available cryptographic IP cores into a single TLS 1.3 protocol engine, including AES256-GCM [11], ECDH and ECDSA [13], HKDF/HMAC/SHA-2 [12], and a TRNG [14].

Interfaces

The interface diagram of XIP7131C is shown in Figure 2. XIP7131C is controlled and configured through a single AXI4-Lite slave interface (`s_axi_csr`) used for command, status and register (CSR) access. Payload data is carried over four independent AXI4-Stream interfaces: an input stream `s_axis_tx_i` carrying plaintext to be encrypted and authenticated, together with the corresponding output stream `m_axis_tx_o` carrying the resulting ciphertext, for the transmit (TX) direction; and an input stream `s_axis_rx_i` carrying ciphertext to be decrypted and authenticated, together with the corresponding output stream `m_axis_rx_o` carrying the resulting plaintext, for the receive (RX) direction.

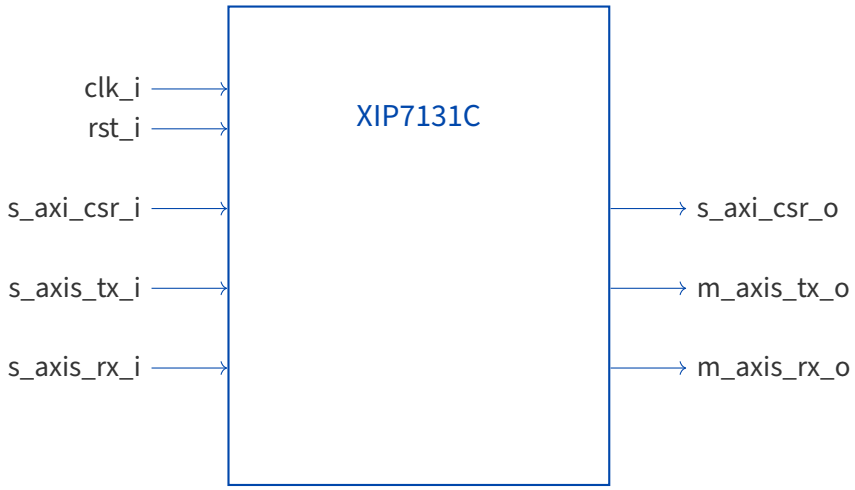

Figure 2: Interface diagram of XIP7131C

Example Use Cases

XIP7131C is well suited for a wide range of critical network applications that require TLS 1.3 protected communication entirely in hardware, including:

- Industrial automation and communications
- Remote management, configuration and control interfaces
- Edge computing
- System-of-Systems communication
- Test & Measurement connectivity
- Networked storage

A typical system integration of XIP7131C is illustrated in Figure 3. Application logic exchanges plaintext with XIP7131C on its secure side, while the TLS 1.3 protected records produced on the insecure side are carried over a full-hardware TCP/UDP/IPv4 stack, such as the Network Protocol Accelerator Platform (NPAP) from Missing Link Electronics [7], and transmitted through an Ethernet MAC. A soft processor supervises both XIP7131C and the protocol stack over AXI4-Lite, so that the complete secure networking datapath is realised in hardware without a software TLS or TCP/IP

stack. Because the records produced by XIP7131C are ordinary TCP payload, the protocol stack transports them unchanged and the record layer stays invisible to the rest of the system. Flows that are not TLS protected are bypassed and pass through XIP7131C unmodified, so a single instance can serve a datapath carrying both protected and unprotected traffic.

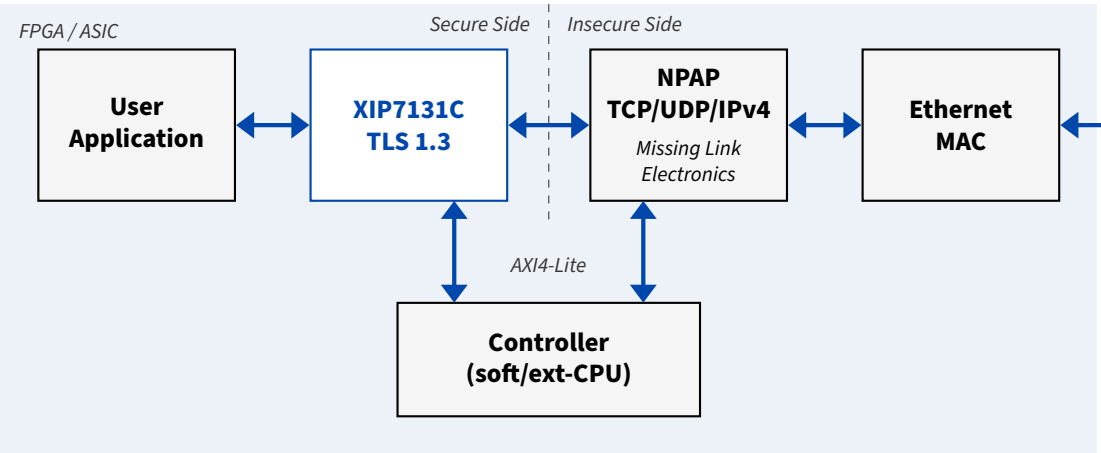

Figure 3: XIP7131C in a full-hardware secure networking datapath

Ordering and Deliverables

Please contact sales@xiphera.com for pricing and your preferred delivery method. XIP7131C can be shipped in a number of formats, including netlist, encrypted, obfuscated or plain text HDL source code. Additionally, compilation scripts, a testbench, and a detailed datasheet including an integration guide can be included depending on the target architecture.

Export Control

XIP7131C protects data confidentiality and is a dual-use product as defined in the Wassenaar Arrangement. Consequently, the export of XIP7131C is controlled by Council Regulation (EC) No 2021/821 and its subsequent changes.

XIP7131C 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 a typical processing time for an export authorization is a few weeks.

About Xiphera

Xiphera specializes in secure and efficient implementations of standardized 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 Ltd.
Metsänpojankuja 1
FIN-02130 Espoo
Finland
sales@xiphera.com
+358 20 730 5252

References

[1] Specification for the Advanced Encryption Standard (AES). Federal Information Processing Standards Publication 197, 2001.

[2] SP 800-56A Rev.3 Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography. Technical report, National Institute of Standards & Technology, Gaithersburg, MD, United States, 2018.

[3] NIST Computer Security Division. FIPS PUB 180-4 Secure Hash Standard (SHS). Technical report, National Institute of Standards & Technology, Gaithersburg, MD, United States, 2015.

[4] NIST Computer Security Division. FIPS PUB 186-5 Digital Signature Standard (DSS). FIPS Publication 186-5, National Institute of Standards & Technology, Gaithersburg, MD, United States, February 2023.

[5] 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.

[6] Dr. Hugo Krawczyk and Pasi Eronen. HMAC-based Extract-and-Expand Key Derivation Function (HKDF). RFC 5869, May 2010.

[7] Missing Link Electronics, Inc. NPAP: Network protocol accelerator platform, full-hardware TCP/UDP/IPv4 stack. `https://www.missinglinkelectronics.com/ip-cores/npap-tcp-udp-ip-stack/`.

[8] Y. Nir and A. Langley. ChaCha20 and Poly1305 for IETF Protocols. RFC 8439, RFC Editor, June 2018.

[9] Eric Rescorla. The Transport Layer Security (TLS) Protocol Version 1.3. RFC 8446, August 2018.

[10] Douglas Stebila, Scott Fluhrer, and Shay Gueron. Hybrid key exchange in TLS 1.3. Internet-Draft draft-ietf-tls-hybrid-design-06, Internet Engineering Task Force, February 2023. Work in Progress.

[11] Xiphera Ltd. XIP1113B: AES256-GCM - Resource Sheet.

[12] Xiphera Ltd. XIP3322B: HKDF/HMAC/SHA-256 - Resource Sheet.

[13] Xiphera Ltd. XIP41x3C: NIST P-224/P-256/P-384/P-521 ECDH+ECDSA - Resource Sheet.

[14] Xiphera Ltd. XIP8001B: TRNG, true random number generator IP core. `https://xiphera.com/wp-content/uploads/XIP8001B_PB.pdf`, 2023. Product Brief, ver. 1.3.