XIPHERA

PEACE OF MIND IN A DANGEROUS WORLD

TLS 1.3

Product code: XIP7131C

Transport Layer Security (TLS) is a cryptographic protocol used for building a secure connection between a client and a server over the Internet. A hardware-based TLS 1.3 implementation enables high-level security in mission-critical industries, ensuring that security-critical operations are entirely self-reliant on hardware, eliminating the need for software. Despite the extensive feature set, Xiphera TLS 1.3 IP cores maintain a compact footprint, making them exceptionally well-suited for high-volume applications.

KEY FEATURES

- Minimal resource requirements
- Optimised performance
- Follows RFC 8446 with selected ciphers
- Powered by AES256-GCM
- Cryptographic operations performed directly in hardware for security and performance
- Hardware-based key management
- Easy system integration
- Vendor agnostic FPGA/ASIC implementation

APPLICATIONS

Versatile solution for critical network applications:

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

TLS 1.3 AES256-GCM

Tailored for every network requirement

The TLS 1.3 IP core is designed to provide robust and efficient security for network communications. This compact solution offers high performance while maintaining minimal resource use, making it the ideal choice for applications where both security and efficiency are essential.

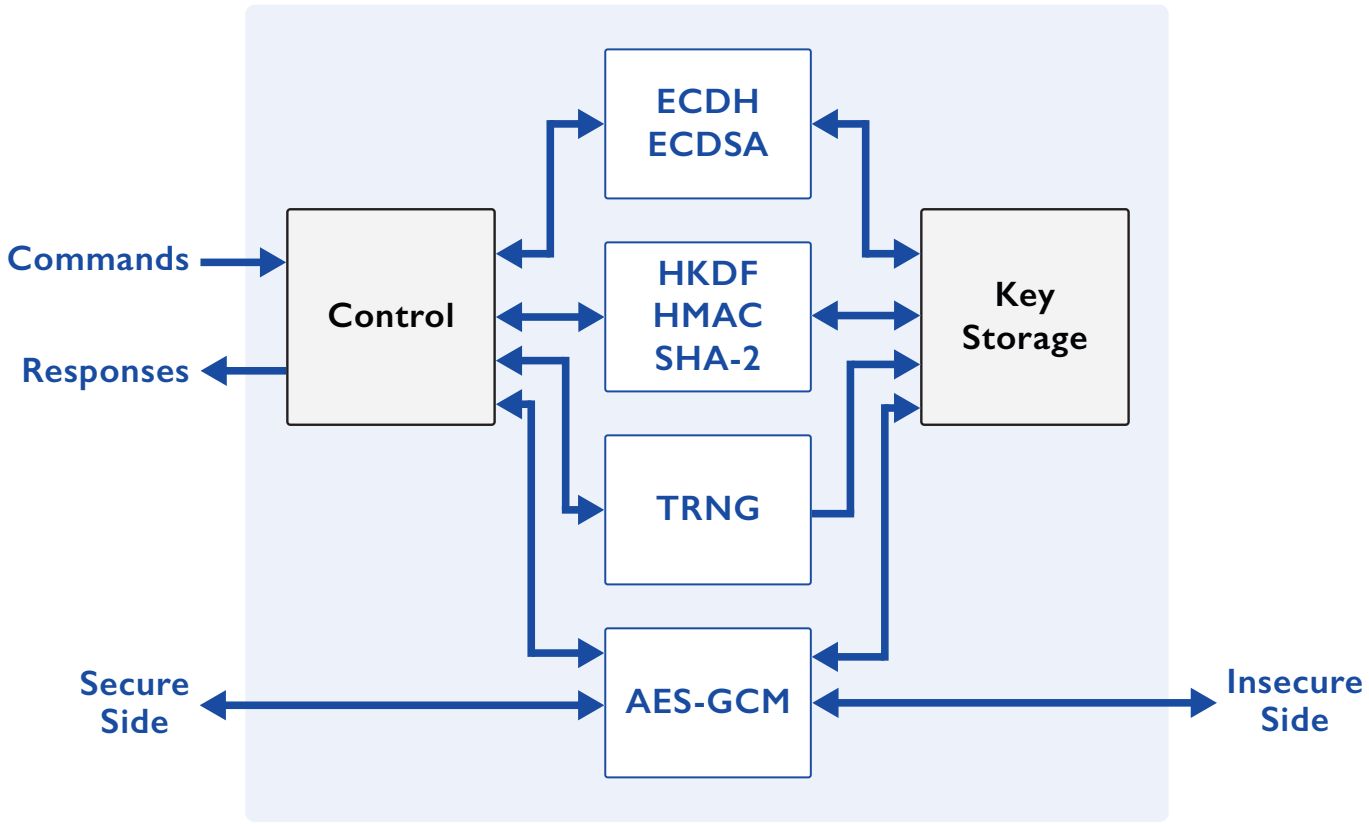
COMPACT

XIP7131C

- Optimised resource use with 8.4kLUTs, excellent fit for high-volume FPGAs
- Over 1 Gbps bulk traffic (client)

XIPHERA

TLS 1.3



Deliverables

✓ Encrypted RTL or source code	✓ Optional netlist
✓ Sample synthesis scripts	✓ Instantiation file
✓ Comprehensive simulation test bench, scripts & guide	✓ Detailed datasheet and integration guide

About Xiphera

Xiphera, Ltd, is a Finnish company designing hardware-based security solutions using standardised cryptographic algorithms. Our product portfolio consists of secure and efficient cryptographic Intellectual Property (IP) cores, designed directly for ASICs and FPGAs. Our strong cryptographic expertise, extensive experience in system design, and deep knowledge in the field of reprogrammable logic enable us to offer our customers peace of mind in a dangerous world.

XIPHERA
PEACE OF MIND IN A DANGEROUS WORLD

Email: sales@xiphera.com
Phone: +358 20 730 5252
Web: www.xiphera.com