Solution Brief

Embedded IoT
Secure Communication

FPGA Hardware-based TLS Security for IoT

Mission critical hardened security for embedded applications using TLS 1.3

Transport Layer Security (TLS) is a cryptographic protocol that provides communication security in IoT applications. Xiphera TLS1.3 intellectual property (IP) on Intel® Edge-Centric FPGAs can enable critical protection of Internet of Things (IoT) devices and the data they produce, process, and transmit, while simultaneously maximizing performance, availability, and ease of use.

The main advantage of FPGA-based security is a hardware-based implementation isolated from any software stacks and operating systems in which most attacks seek to exploit vulnerabilities. The additional technical advantages of FPGA-based implementation of cryptography include:

- Algorithm and protocol agility and updatability
- Possibility to utilize built-in FPGA security features:
  - Encrypted and authenticated configuration
  - Partial reconfiguration on select Cyclone® V FPGA implementations eases in-field updates
  - Design methods to achieve design separation of secure and non-secure in hardware
- Performance boost of security functions

Solution Overview

- Implements physically separated cryptography and key storage
- IP implements secure connection setup and key management
- Full isolation of cryptographic keys minimizes attack vulnerabilities
- Optimized for low footprint applications, targeting Intel® MAX® and Intel® Cyclone® FPGAs
- The TLS 1.3 IP core can retrofit into existing FPGA-based solutions
- Higher encryption performance (throughput and latency) and stronger protection against attacks vs software-based TLS
- Independence from software tool flow vulnerabilities

Authors

Mark Jervis
Solutions Architect
Industrial and Automotive BU
Intel Programmable Solutions Group

Customer Benefits

- Turn-key TLS security solution ready to integrate into your FPGA-based embedded design
- Hardware-based implementation, as mandated by some government and industry security standards
- Flexible and updatable cryptographic functions for long in-field lifetimes
- Meet IEC 62443 requirements for embedded designs
- FPGA flexibility enables customizable algorithms to allow future-proofing designs to support Post-Quantum Cryptography (PQC)
- TLS IP running in the FPGA logic allows you to maximize application performance

Target Application

- Industrial edge IoT and gateway applications
- Industrial IoT, manufacturing, and process automation for anomaly detection and predictive maintenance
- Smart city infrastructure, building environmental sensing and energy optimization
- Government and military secure communications
- Remote monitoring and control
- Medical devices for real-time sensing and machine learning-based diagnosis
- Test and measurement connected devices
- Transportation, monitoring, and traffic flow optimization

Learn More

- Edge-Centric Overview Page
- FPGA-based security solutions white paper
- Xiphera TLS IP
- Contact Xiphera: info@xiphera.com

ss-1135-1.0