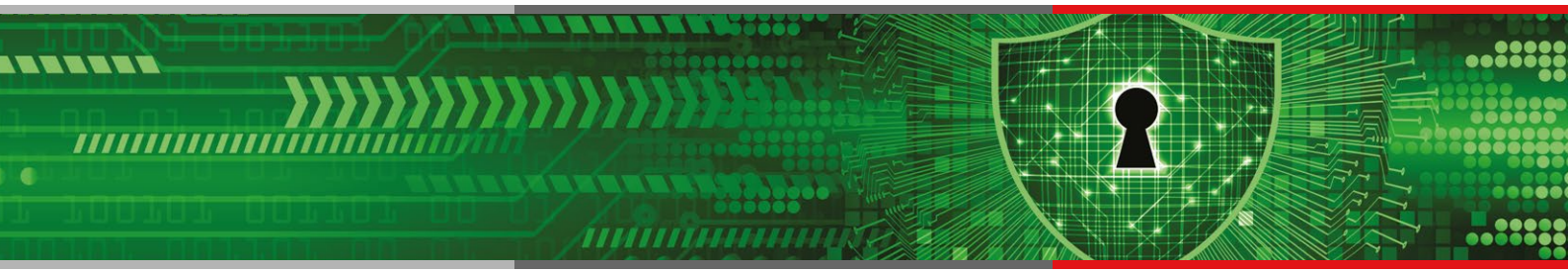
SILEX INSIGHT

Product sheet
BA452

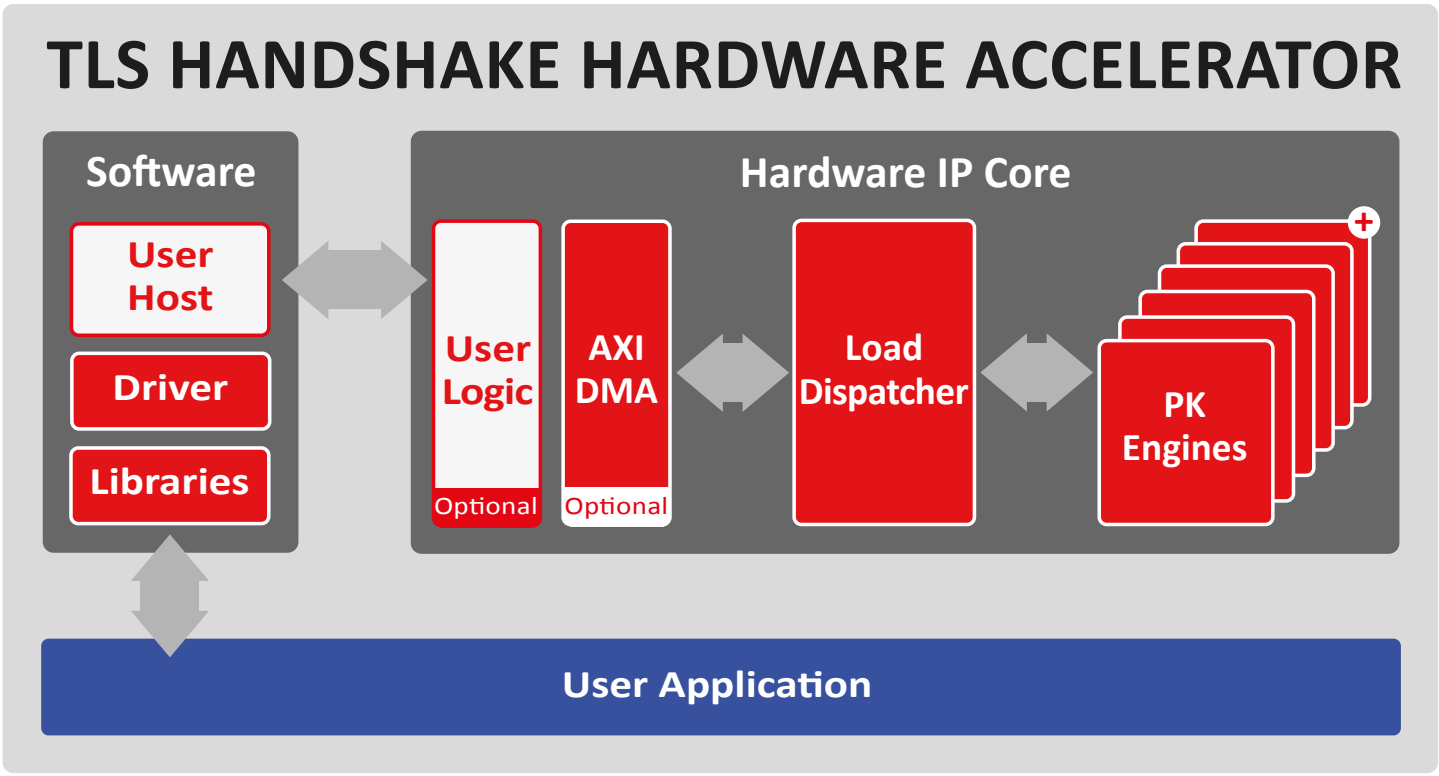


TLS HANDSHAKE HARDWARE ACCELERATOR

The TLS handshake hardware accelerator is a secure connection engine that can be used to offload the compute intensive Public Key operations (Diffie-Hellman, Signature Generation and Verification).

It combines a load dispatcher and a configurable amount of instances of the Public Key Crypto Engine (BA414EP) benefiting from all features supported (i.e. RSA/DH/DHE and ECDSA/ECDH/ECDHE/X.25519/X.448 and more). The efficient dispatching to several tenths of BA414EP instances helps reaching maximum system performance.

This IP is made of a core and optional modules to connect the core to standard interfaces (PCIe, AXI_DMA...). In addition our drivers have an asynchronous API (or non-blocking API) which are integrated in OpenSSL Async.



Features

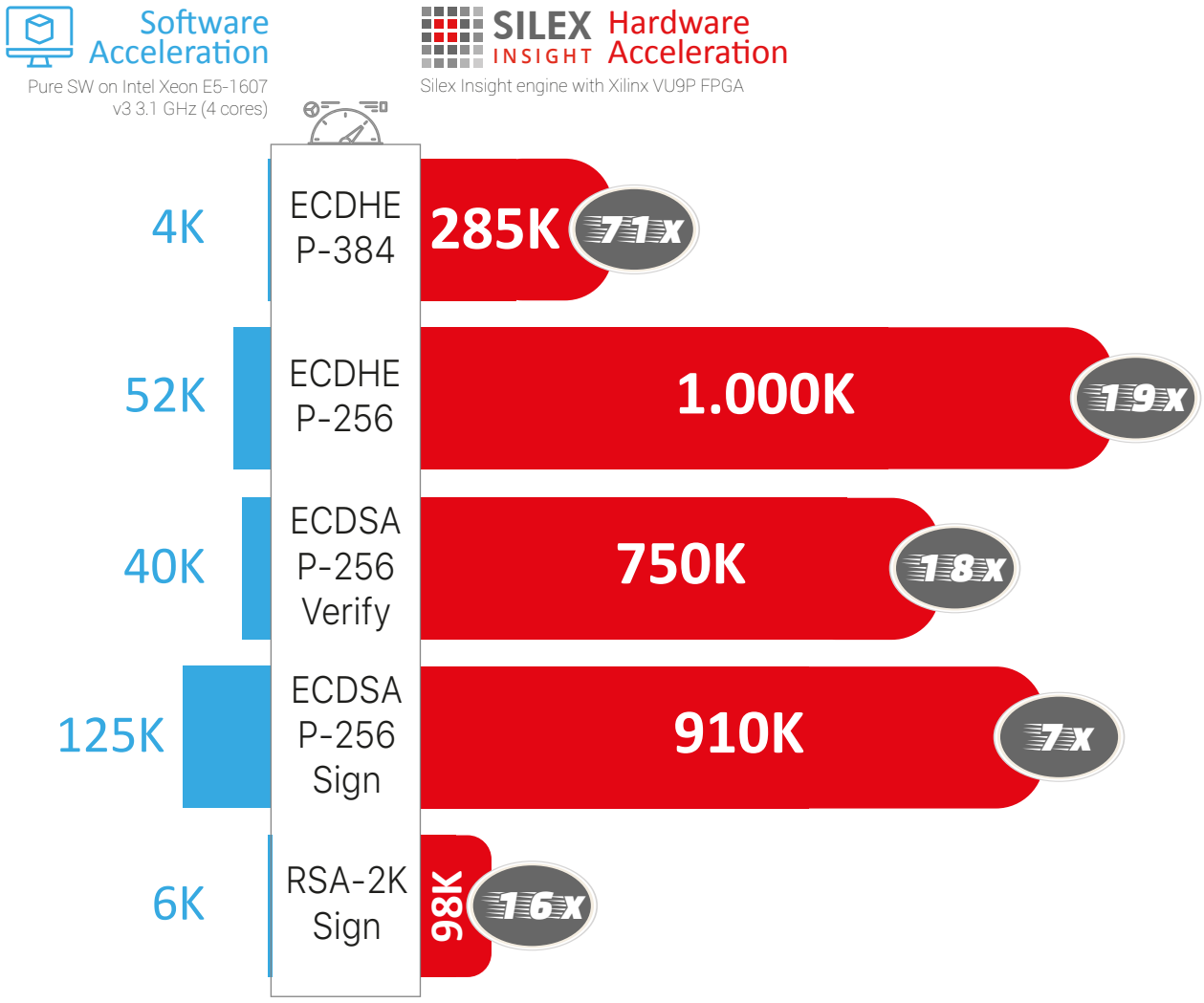
- Scalable architecture
- OpenSSL integration (optional)
- DTA protection (DPA optional)
- Custom operations possible on request
- High performance on off-the-shelf FPGA
- Plug'n Play integration with PCIe (Xilinx Alveo board)
- Wide variety of crypto algorithms supported:
  - RSA with and without CRT
  - Elliptic Curve Cryptography(ECC)
  - Diffie-Hellman (D-H and ECDH) Key Exchange
  - Digital Signature Algorithm(DSA) & Elliptic Curve Digital Signature Algorithm (ECDSA, EC-KCDSA & EdDSA)
  - X.25519/X.448
  - SM2
  - Any other crypto algorithm can be supported
- ASIC and FPGA (incl. UltraScale+ & Versal)

Applications

- Cloud computing
- Data center
- HSM
- Firewall
- IKE-TLS/SSL connection engine
- Blockchain transactions

ALGORITHMIC PERFORMANCE WITH OpenSSL SPEED

Using OpenSSL v1.1.1G /OpenSSL speed command



This comparison has been done using FPGA. If ASIC is used the hardware can run up to 3x higher.

Implementation aspects

The TLS handshake hardware accelerator IP core is easily portable to ASIC and FPGA. It supports a wide range of applications on various technologies. The unique architecture offers a high level of scalability, enabling a trade-off between throughput, area and latency.

Deliverables

- Netlist or RTL
- SW drivers (Linux)
- Scripts for synthesis & STA
- Self-checking RTL test-bench based on referenced vectors
- Documentation

For more detailed information about our **Public Key Crypto Engine (BA414EP)**, please see our dedicated product sheet.

Silex Insight
Rue Emile Francqui 11,
1435 Mont-Saint-Guibert, Belgium

Tel: +32 10 45 49 04
E-mail: contact@silexinsight.com
Web: www.silexinsight.com