SILEX INSIGHT

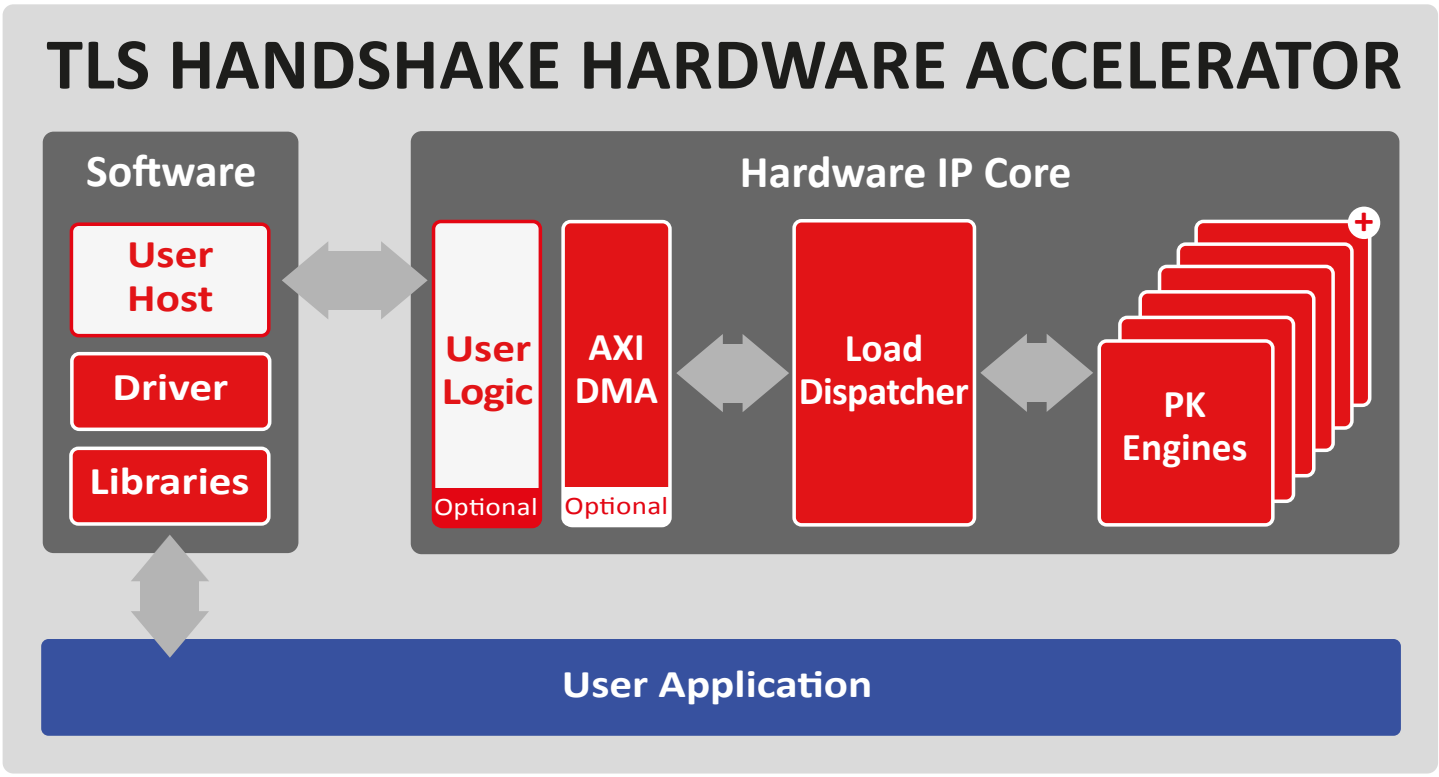
Product sheet
BA452

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.



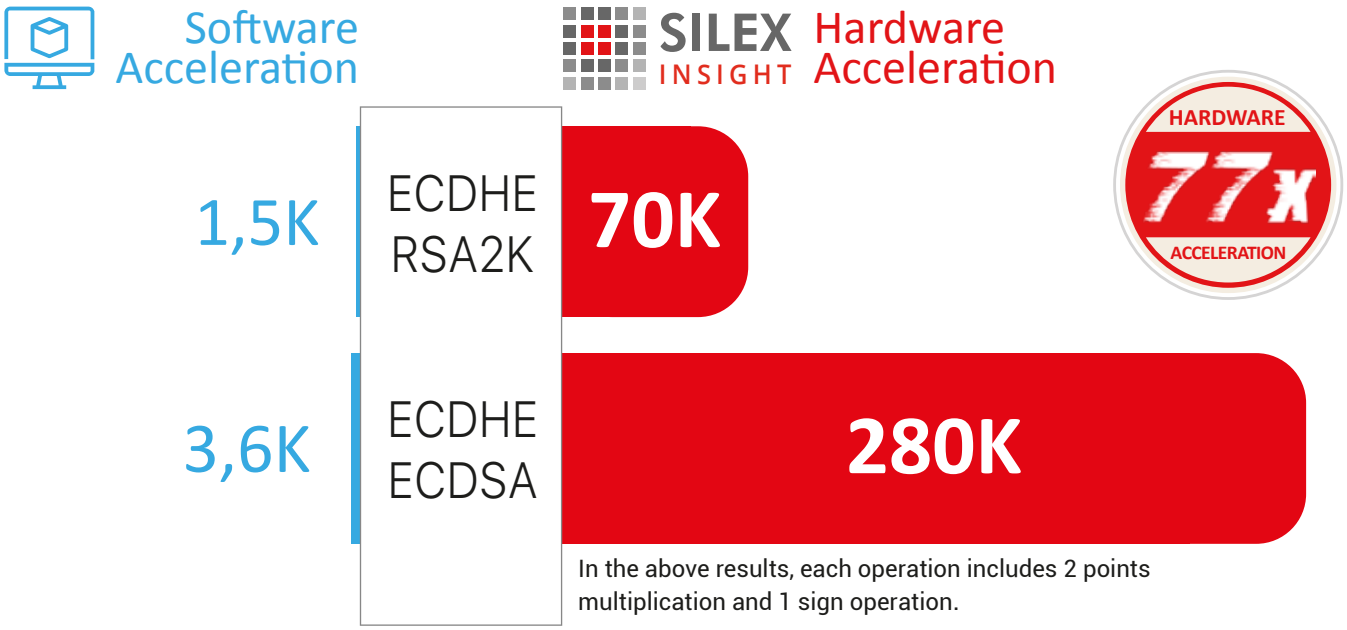
Features

- RSA, ECC and more
  - RSA/DH/DHE
  - ECDSA/ECDH/ECDHE
  - X.25519/X.448
  - SM2
- > 1 GHz in 16nm
- 400-500 MHz on mid-range/ high-end FPGA
- Very high performance on off-the-shelf FPGA

Applications

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

TLS connection performance (Ops/s)



In the above results, each operation includes 2 points multiplication and 1 sign operation.

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