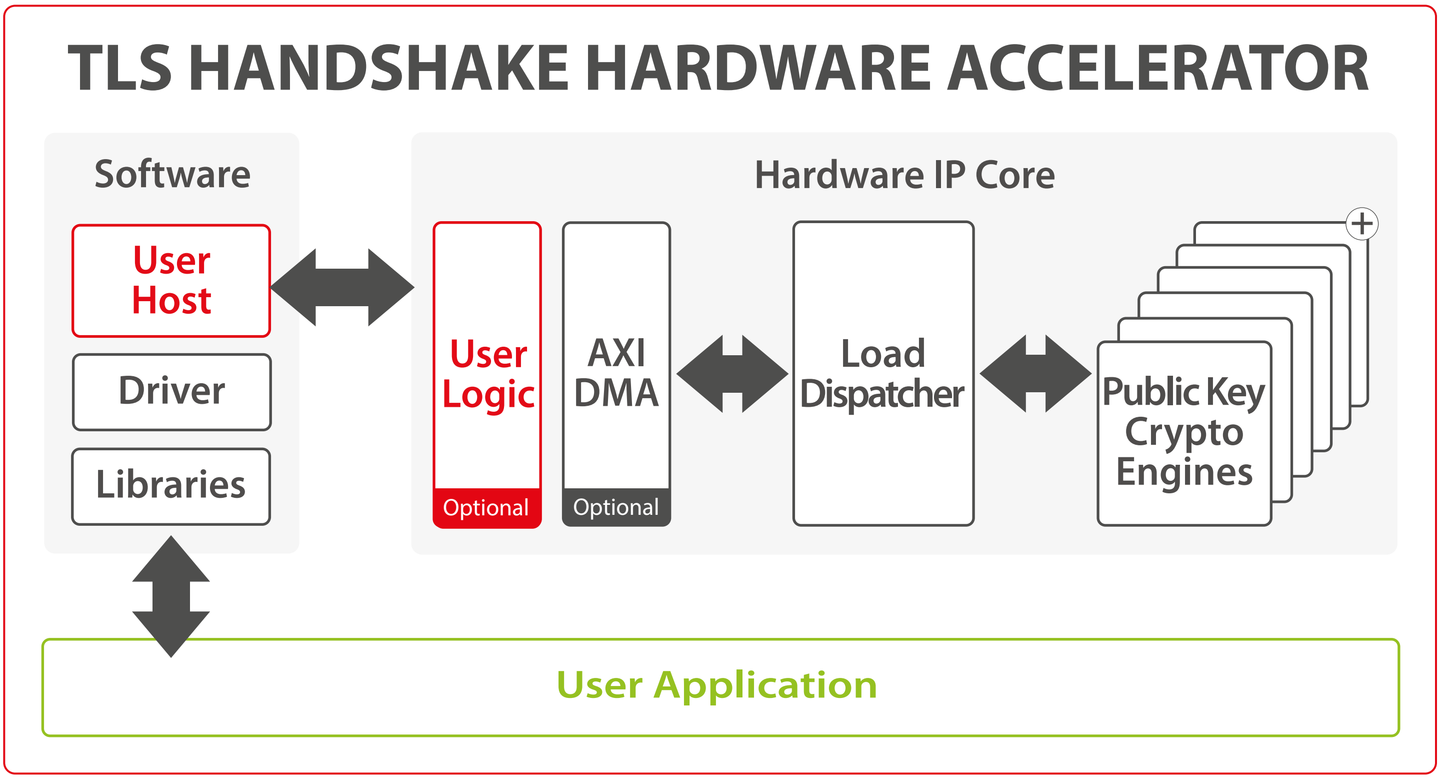
Securyzr™ > Securyzr™ Secure HW Solutions > Securyzr™ Secure Protocol Engines > SCZ_SP_BA452

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 Key Exchange, Signature Generation and Verification).

It combines a load dispatcher and a configurable amount of instances of the Public Key Crypto Engine (SCZ_IP_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 dozens of SCZ_IP_BA414EP instances helps reach maximum system performance.

This IP is made of a core and optional modules aiming at connecting the core to standard interfaces (PCIe, DMA, AXI bus). In addition, device drivers have an asynchronous API (or non-blocking API) which is integrated in OpenSSL Async.



Features

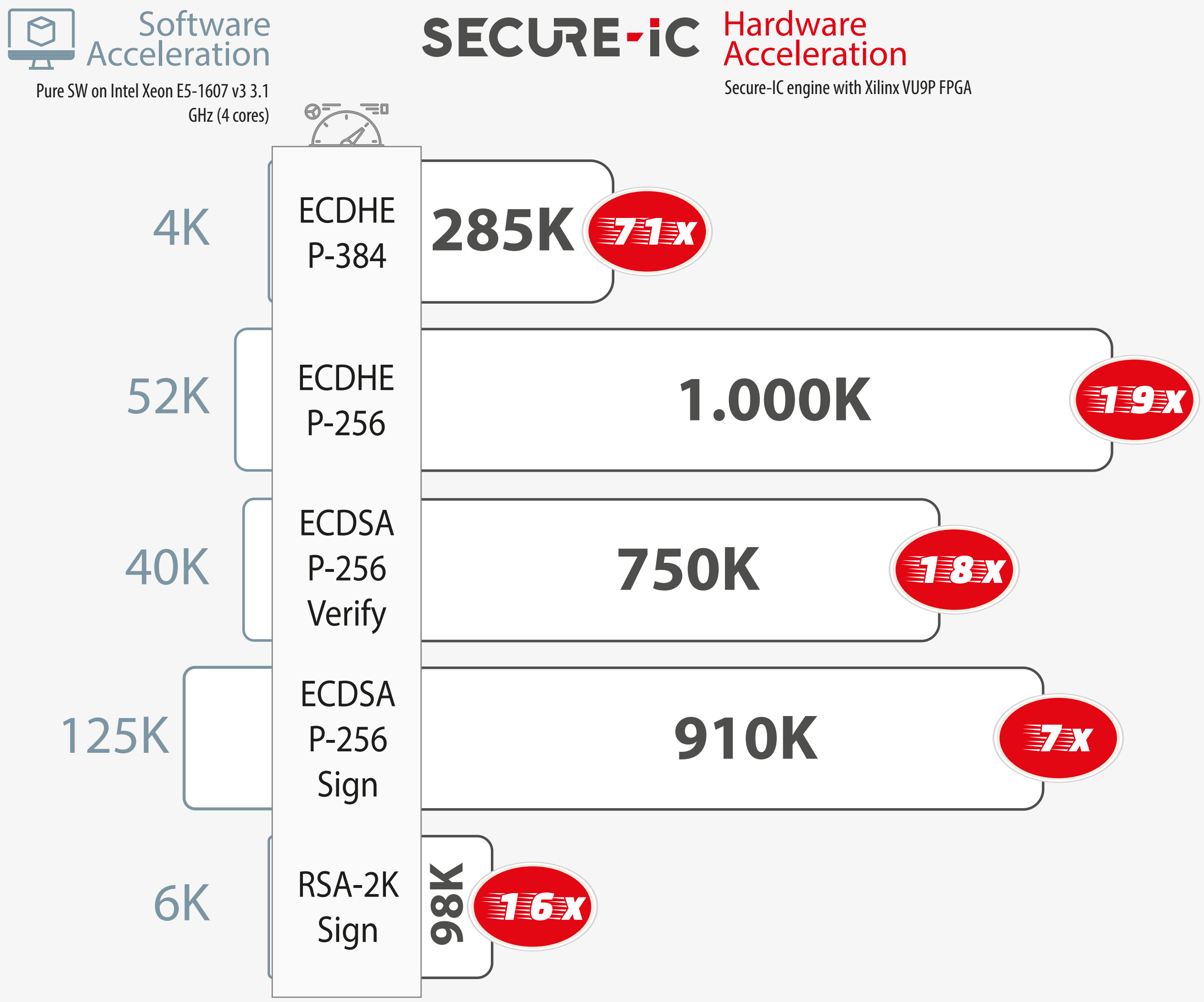
- Scalable architecture
- OpenSSL integration (optional)
- Custom operations possible on request
- High performance on off-the-shelf FPGA
- Plug'n Play integration with PCIe (e.g., Xilinx Alveo board)
- ASIC and FPGA (incl. UltraScale+ & Versal)
- Wide variety of crypto algorithms supported:
  - RSA 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

Applications

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

ALGORITHMIC PERFORMANCE (OPS/S) 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 faster.

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. For more detailed information about our Public Key Crypto Engine (SCZ_IP_BA414EP), please see our dedicated product sheet.

Deliverables

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

V1.2

SECURE-IC
THE SECURITY SCIENCE COMPANY

HEADQUARTERS
Digital Park B - ZAC Atalante Via Silva
801 avenue des Champs Blancs
35510 Cesson-Sévigné - France
+33 (0)2 99 12 18 72 - contact@secure-ic.com

EMEA
sales-EMEA@secure-ic.com

AMERICAS
sales-US@secure-ic.com

APAC
sales-APAC@secure-ic.com

JAPAN
sales-JAPAN@secure-ic.com

CHINA
sales-CHINA@secure-ic.com

CONTACT US
www.secure-ic.com