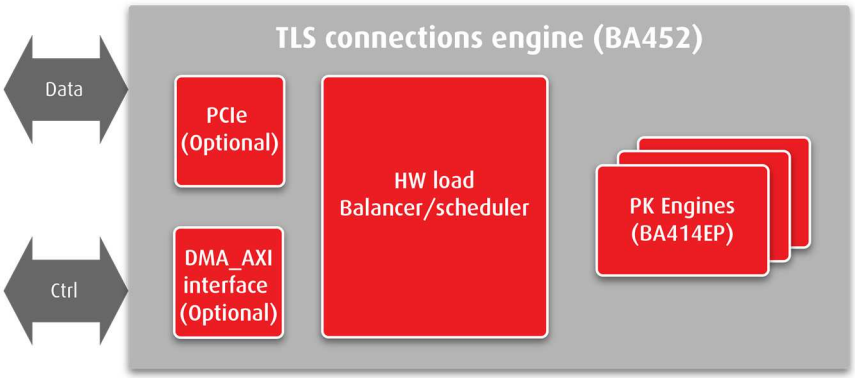
Secure connection engine

BA452
Product sheet

The BA452 is a secure connection engine that can be used to off-load the compute intensive Public Key operations (Diffie-Helmann, Signature Generation and Verification).

It combines a load balancer and a configurable amount of instances of the BA414EP Public-Key Cryptography engine benefiting from all features supported in the BA414EP (i.e. RSA/DH/DSA and ECC/ECDSA/ECDH/X.25519/X.448 and more). This module enables to efficiently obtain maximum system performance with several tenths of BA414EP instances being scheduled efficiently.

The BA452 IP is made of a core and optional modules to connect the core to standard interfaces (PCIe, AXI_DMA…).



Features

- RSA, ECC and more
  - ECDH, ECDSA
  - DSA, DH, RSA
  - X.25519, X.448
  - SM2
- > 1 GHz in ASIC 16 nm
- 400-500 MHz on mid-range/high-end FPGA
- Very high performance on off-the-shelf FPGA
- 1300K ECC P-256/s
- 125K RSA-2K/s

Applications

- Cloud computing
- Data Center
- IKE - TLS/SSL connection engine
- Crypto currency transactions (Bitcoin, others…)
- V2X (cloud side)

Implementation aspects

The BA452 IP core is easily portable to ASIC and FPGA. It supports a wide range of applications on various technologies. The unique architecture enables 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 test-bench based on referenced vectors
- Documentation