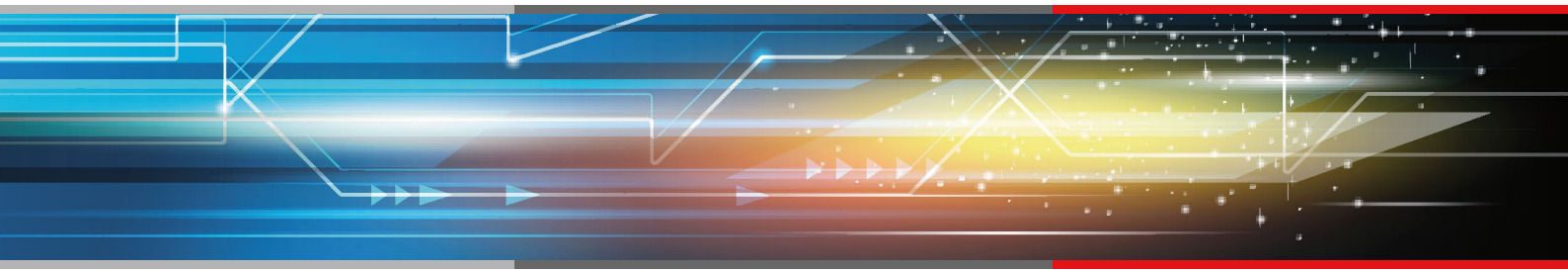
SILEX INSIGHT

Product sheet
BA453



NETWORK SECURITY CRYPTO ACCELERATOR

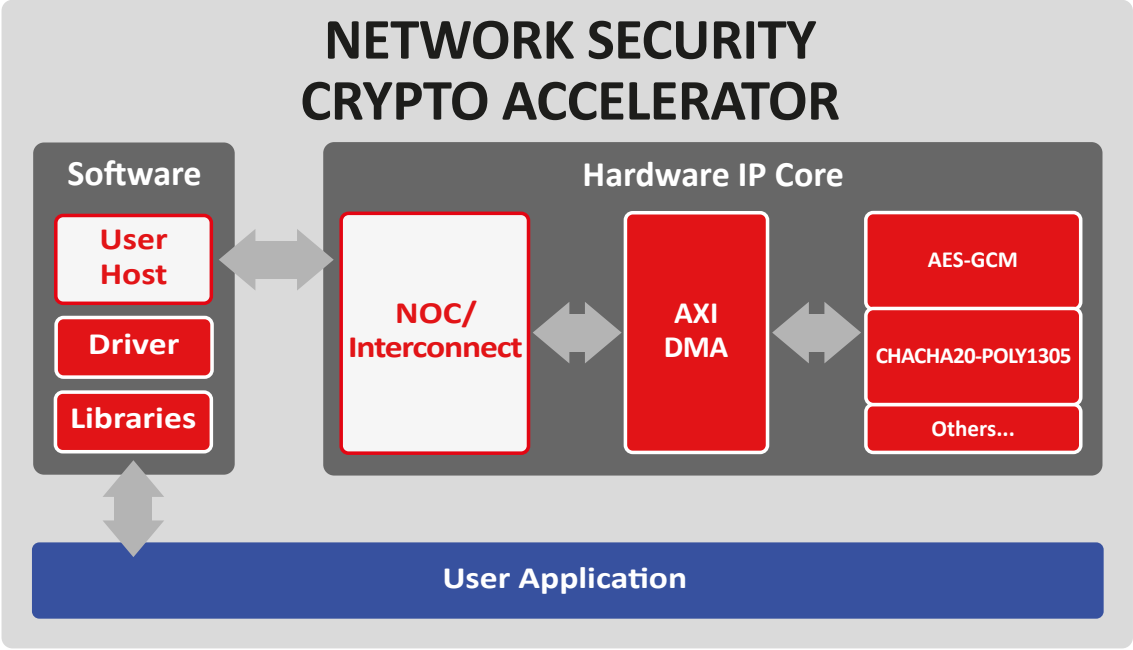
The Network Security Crypto Accelerator is a hardware IP core platform that accelerates cryptographic operations in System-on-Chip (SoC) environment on FPGA or ASIC.

This IP is used to accelerate/offload MACsec, IPsec, VPN, TLS/SSL, disk encryption, or any other custom application, requiring symmetric cryptography algorithms. The operations are efficiently offloaded via a built-in scatter-gather DMA optimized to handle networks packets of any size.

The Network Security Crypto Accelerator can also be combined with our Root of Trust eSecure module to form a complete secure enclave, that will handle the keys without exposing them to the software.

General description

The platform integrates your desired selection of our cryptographic IP cores, a DMA and software layers providing a complete solution.



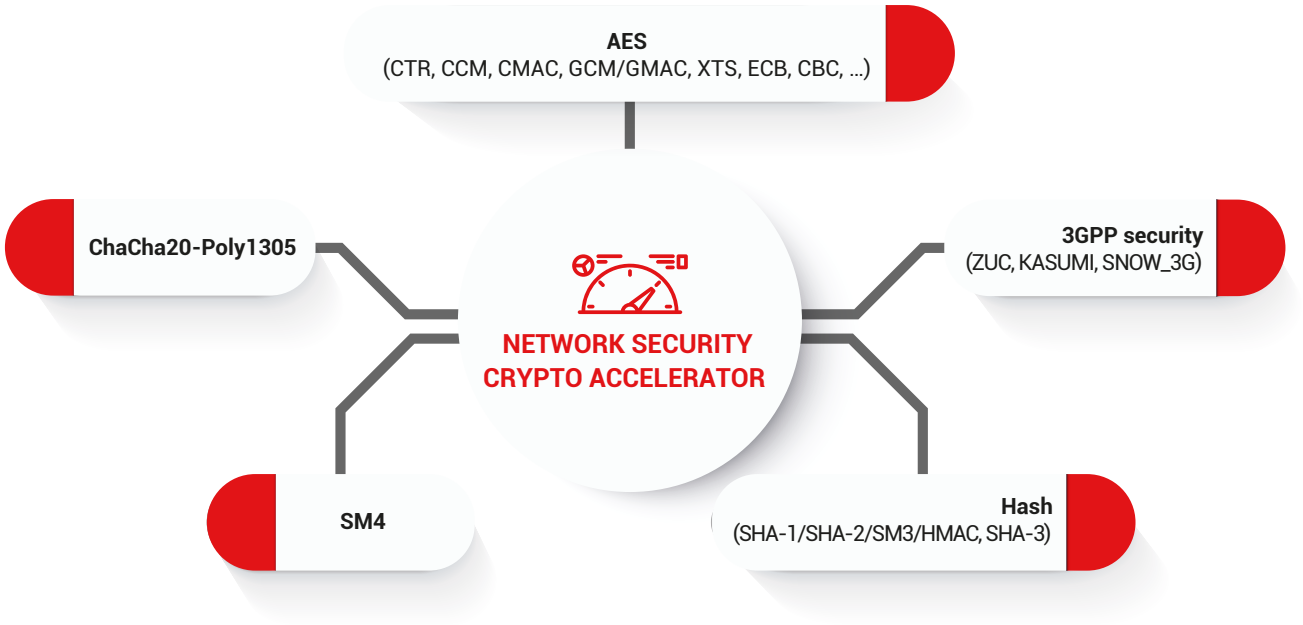
Features

- Scalable architecture and crypto engines for optimal performance/resource usage
- Configurable for perfect application fit
- 100% CPU offload with low latency and high throughput
- Optional DPA countermeasures for AES and SM4
- Full software/driver support
  - Linux drivers (Crypto API integration)
- Easy integration
  - AXI interface
- Low power
- Can use keys (from eSecure or others) hidden from CPU

Applications

- Secure communication (TLS, MACsec, IPSec, ...)
- Secure storage

The following cryptographic engines can be selected to be integrated:



Software Interfacing

The software API and drivers interfaces with Crypto API from the Linux OS.

Deliverables

- Netlist or RTL
- SW drivers (Linux)
- Scripts for implementations
- Self-checking RTL test-bench based on FIPS vectors
- Documentation

Other high performance IP blocks to offload network & security processing

Can be used in combination with the Network Security Crypto Accelerator

We're offering the key components to boost your data center, including one of the fastest SSL/TLS handshaking engines for asymmetric operations in the industry and ultra-high performance MACsec and IPsec processing.

TLS Handshake Hardware Accelerator (BA452)

An asymmetric secure connection engine that can be used to offload the compute intensive Public Key operations.

MACsec Engine (BA451)

Providing connectionless data integrity, data origin authenticity and confidentiality on OSI layer 2.

IPsec Engine (BA454)

Providing confidentiality, connectionless data integrity, data-origin authentication and replay protection on OSI layer 3.

SILEX INSIGHT

Product sheet

BA453 - Network Security Crypto Accelerator

V1.1

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