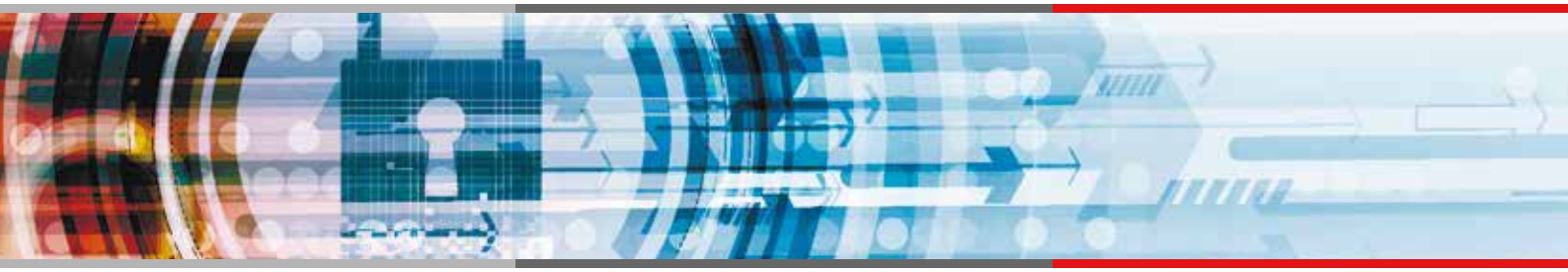
SILEX INSIGHT

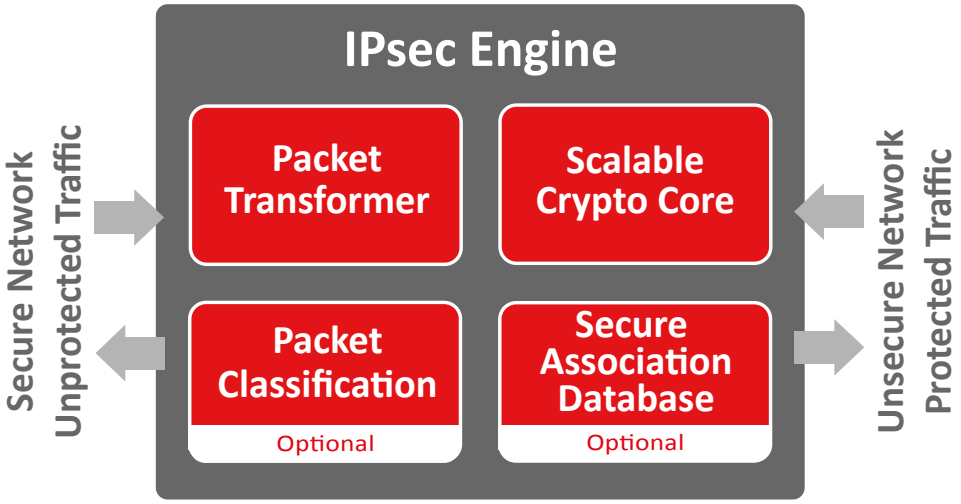
Product sheet
BA454



IPsec ENGINE

The IPsec Engine implements RFC4301 and other relevant RFCs, providing confidentiality, connectionless data integrity, data-origin authentication and replay protection on OSI layer 3.

The scalable architecture provides low-latency, line rate acceleration of packet encapsulation, encryption and replay protection. Its modular design not only gives the ability to choose between different cryptographic algorithms, but also provides fine-grained control on classification features, packet formats, and more. Integration with a wide range of performance or area-optimized cryptographic IP cores allows unrivalled trade-off possibilities between throughput, area and latency.



Features

- ASIC and FPGA
- Can aggregate several 10, 40 or 100 GbE link
- Throughput from 1 Gbps up to 100 Gbps
- Compliant with RFC 4106, 4301, 4303, 7634
- Supports AES-GCM-128/256, AES-CBC/SHA-2, ChaCha20 Poly1305
- 32 to 1024 bits datapath
- ESP encapsulation/decapsulation
- UDP encapsulation
- Byte lifetime counters
- Generic interface to TCAM
- Supports IPv4 and IPv6
- 5-tuple classification
- Bypass mode
- Data interface: AMBA 4 AXI-Stream
- Control interface: AMBA 4 APB

Applications

- Cloud computing
- Data center
- Edge router
- Edge networking for IoT data aggregation

Implementation aspects

At its very core, the IPsec Engine is completely technology-agnostic and can be integrated in a wide range of FPGA and ASIC technologies. On FPGA, the engine can use vendor-specific optimizations to reach very high throughput goals.

Deliverables

- Netlist or RTL
- Scripts for synthesis & STA
- Self-checking RTL test-bench on referenced vectors
- Documentation

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