Securing the connected world

Security acceleration for cloud computing/data centers

SILEX INSIGHT

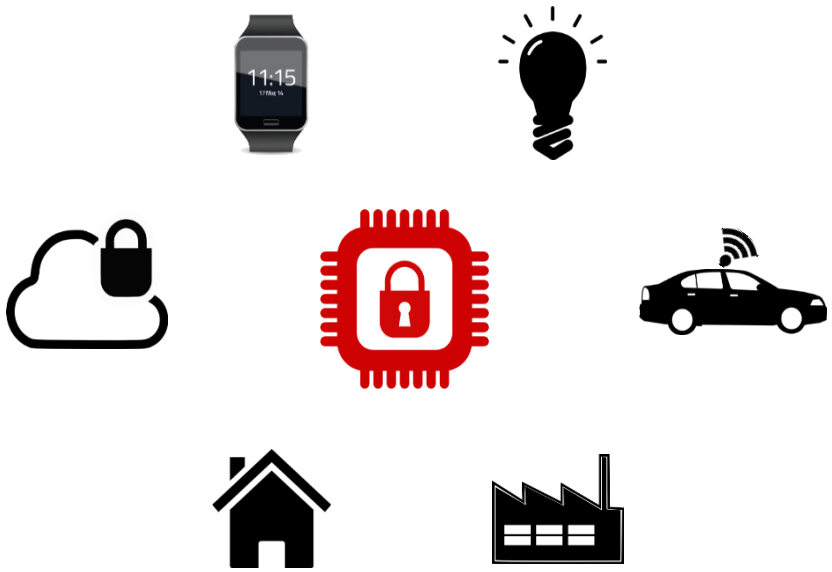
Company history

- 1991: Founded as ASIC design house in Louvain-la-Neuve, Belgium
- 1995: Becomes part of the Barco group.
- 1999: 1st SoC development for payment terminal
- 2003: Introduction of JPEG2000 IP cores for FPGAs
- 2011: Introduction of Public Key and AES cryptographic IP cores
- 2015: Technology & Engineering Emmy Award for J2K Interop
- 2016: Introduction of VIPER: HDMI over IP OEM board
- 2016: Introduction of eSecure: Embedded Security IP
- 2018: Barco Silex becomes Silex Insight and part of the Vehold group
- Silex Insight today:
  - Staff of 35
  - ISO 9001-2008

SILEX INSIGHT

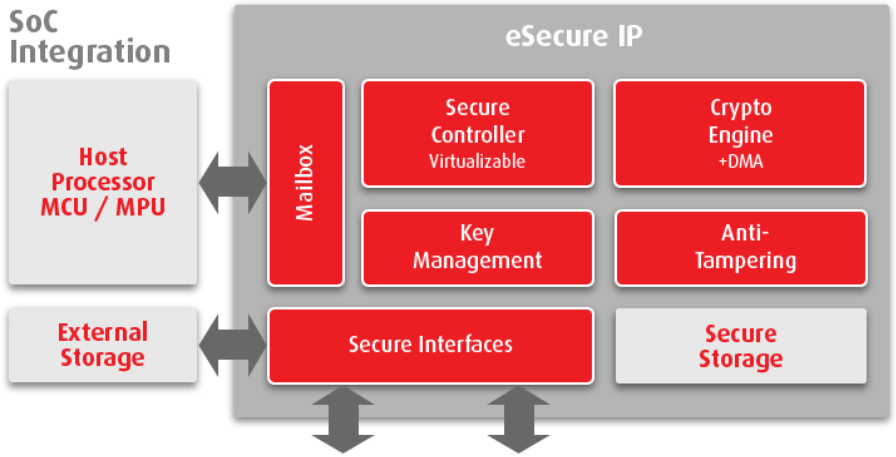
Security markets/applications

- End-point, edge computing, data center



Security IP products overview

- eSecure (HW Root Of Trust, Security Enclave)
  - Secure Boot
  - Secure Debugging
  - Secure Key Storage
  - Device Authentication
  - Anti-tampering – Side Channel Attack protection
  - PUF available
  - Low power features (retention, power down)
  - Evita compliant – Crypto Driver API from AUTOSAR for host library
  - Several processors integrated
    - RISC-V Controller (from various partners)
    - ARM
    - MIPS
  - Wide range of cryptographic algorithms
  - **Silicon proven**
- Applications: Automotive, Industrial, Cloud computing, IoT end Node device, Wireless communications



SILEX INSIGHT

Security IP products overview

- **MACSec packet processor 400/800 Gbps – Cloud computing**
- **IPSec packet processor 100 Gbps – Cloud computing**
  - IPv4/IPv6
  - AES-GCM, Chacha20Poly1305
- **Multi PK engine – Cloud computing, Blockchain**
  - **TLS/SSL connections offloading co-processor for TLS 1.2 and 1.3**
  - Crypto currency transaction
  - V2x certificate generation
- Bus Encryption protecting DDR content
- In line decryptor
- Crypto-Coprocessor

- Customization and design services on the security IP products

SILEX INSIGHT

Supported Cryptographic algorithms

- Asymmetric algorithms
  - RSA/DH/DSA/CRT/ECC/ECDSA/ECDH
    - ECC Curves: NIST, Brainpool, Koblitz, Montgomery, Edwards and others…
  - Apple HomeKit/TLS1.3: Curve25519, EdDSA/Ed448, SRP
  - Thread Protocol: J-PAKE
  - Rabin-Miller (primality check) and Key Generation
  - SM2, Ed448, EC-KCDSA, ECIES, ECMQV
- Symmetric algorithms
  - AES supporting all modes (GCM, CCM, CFB, CBC…)
  - Very High performance AES-GCM/CTR/XTS > 400 Gbps
  - 3GPP algorithms (Snow3G, Kasumi, ZUC)
  - Chacha20_poly1305 – TLS 1.3/Apple HomeKit
  - Very High performance Chacha20_poly1305 > 400 Gbps
  - SHA1/2, SM3
  - SHA-3
  - SM4
  - 3-DES core
- Random Number Generators
  - TRNG (NIST 800-90B and AIS-31)
  - DRBG (NIST 800-90A compliant)

- Unrivalled performances & trade-off performances/area
- Very high level of scalability and flexibility
- Associated Bare-Metal Drivers – Integration into lightweight TLS/DTLS lib
- All cores share the same AMBA interface
  - AXI4 stream
  - AHB/AXI master
  - Embedded DMA for symmetric algorithms
- FIPS 140-2 (level 3/4) / PCI Certification

SILEX INSIGHT

Connected world

- Data center challenges
  - High throughput secure data processing
  - High performance secure connection engine
  - Requires HW offloading to ASIC or FPGA
    - Reduce power consumption
    - Increase performance
    - Offload processor

SILEX INSIGHT

High Perf security protocols

- IPSec: todays requirements can go up to 100 Gbps
- MACSec: todays requirements can go up to 400/800 Gbps
- TLS/SSL connections offloading: requires several 10-Ks connections/s

IPsec/MACsec

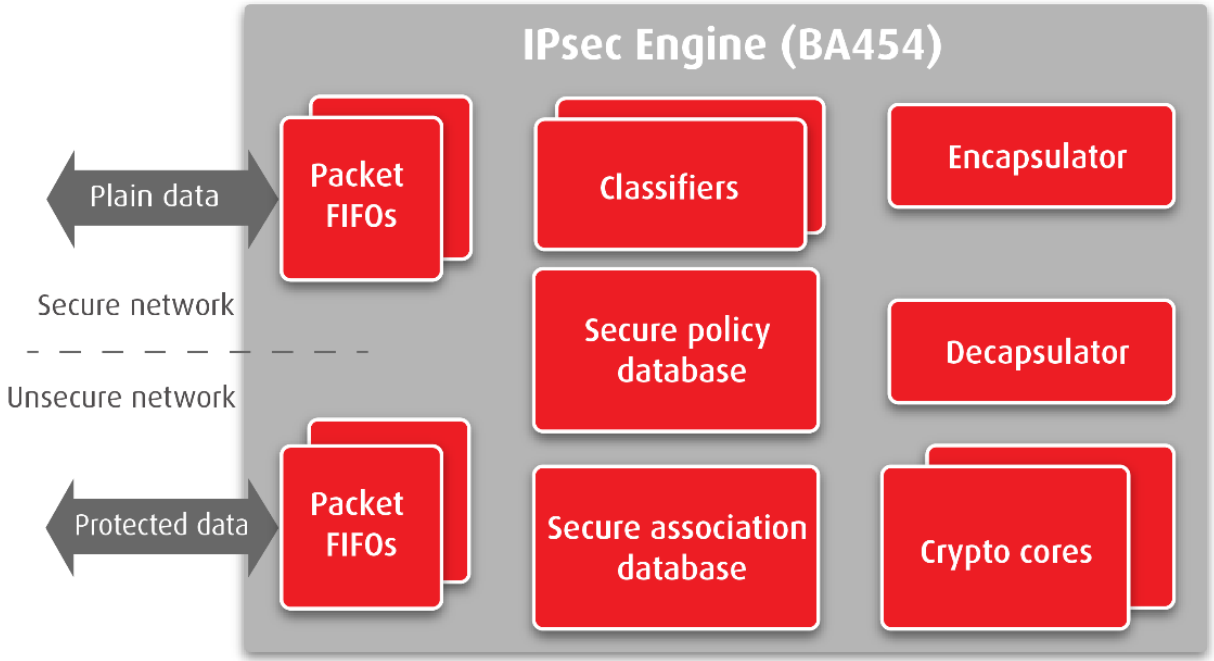
- Data transfer:
  - Source authentication
  - Data integrity
  - Confidentiality

→ Ipsec/MACsec is the transport security protocol of choice

  - Software implementations not well suited
    - timing-critical
    - high-throughput applications
    - HW offloading required

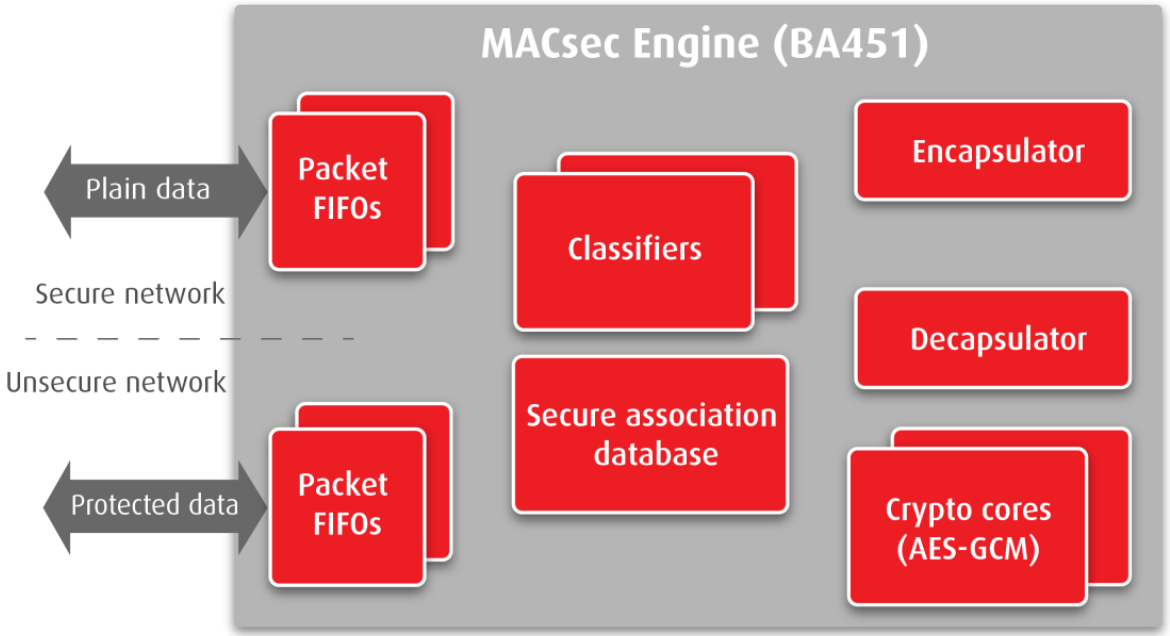
IPSec

- Scalable solution going up to 100 Gbps
- Cryptography algorithms: AES-GCM / Chacha20Poly1305
- Tunnel Mode
- Classification
- ESP encapsulation
- Key size up to 256 bits
- IPv4/IPv6



MACsec

- MACSec Features:
  - Datapath from 128 to 1024 bits
  - Cryptography: AES-GCM-128/256, AES-GCM-XPN-128/256
  - SecTag encapsulation/decaspulation
  - ICV calculation/checking
  - Interface to TCAM
  - Classification
  - Scalable solution: from 10 Gbps to 800 Gbps



SILEX INSIGHT

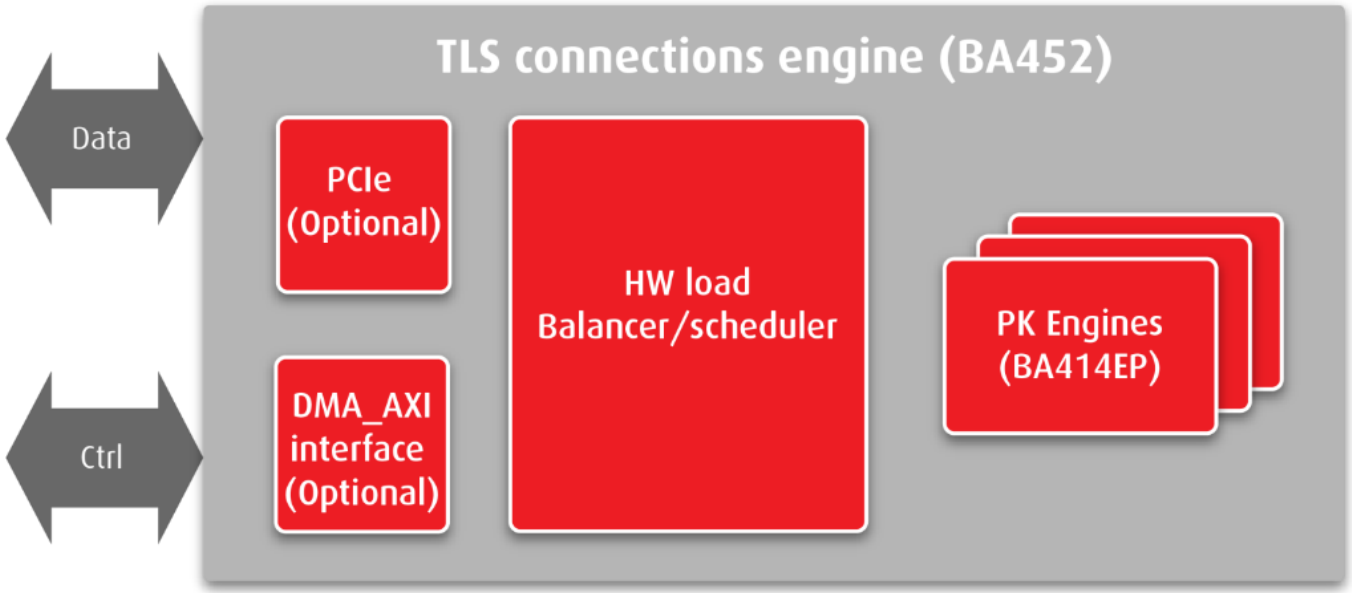
Secure connection engine

- Secure connections
  - TLS/SSL connections
  - Requires compute intensive asymmetric cryptography
  - Software implementations not well suited
    - high number of connections/sec (PK operations)
    - HW offloading required

SILEX INSIGHT

TLS/SSL connection engine

- TLS/SSL connections offloading
  - Several tenths of thousands connections per second
  - Support for TLS 1.2/1.3 algorithms (RSA, ECC NIST/Brainpool/X.25519,X.448/EdDSA,Ed448 and others)
  - Can be implemented in FPGA and ASIC
  - several 10k's TLS/SSL connections per second
  - several hundred thousand ECC P-256 operation per second
  - Above 1Ghz on latest ASIC technology, and 600/700 MHz on latest FPGA
  - HW load balancer schedules optimal use of high performance PK engines



SILEX INSIGHT

Needs and benefits

- HW IPsec/MACsec engine
  - Very high throughput (800Gbps with one engine)
  - Host CPU is free for other critical tasks
  - Improved security
- HW TLS/SSL connection engine
  - Several 10K operations/sec (sign and verify)
  - Host CPU is free for other critical tasks
- FPGA availability in data centers allows for cheap but very efficient implementation