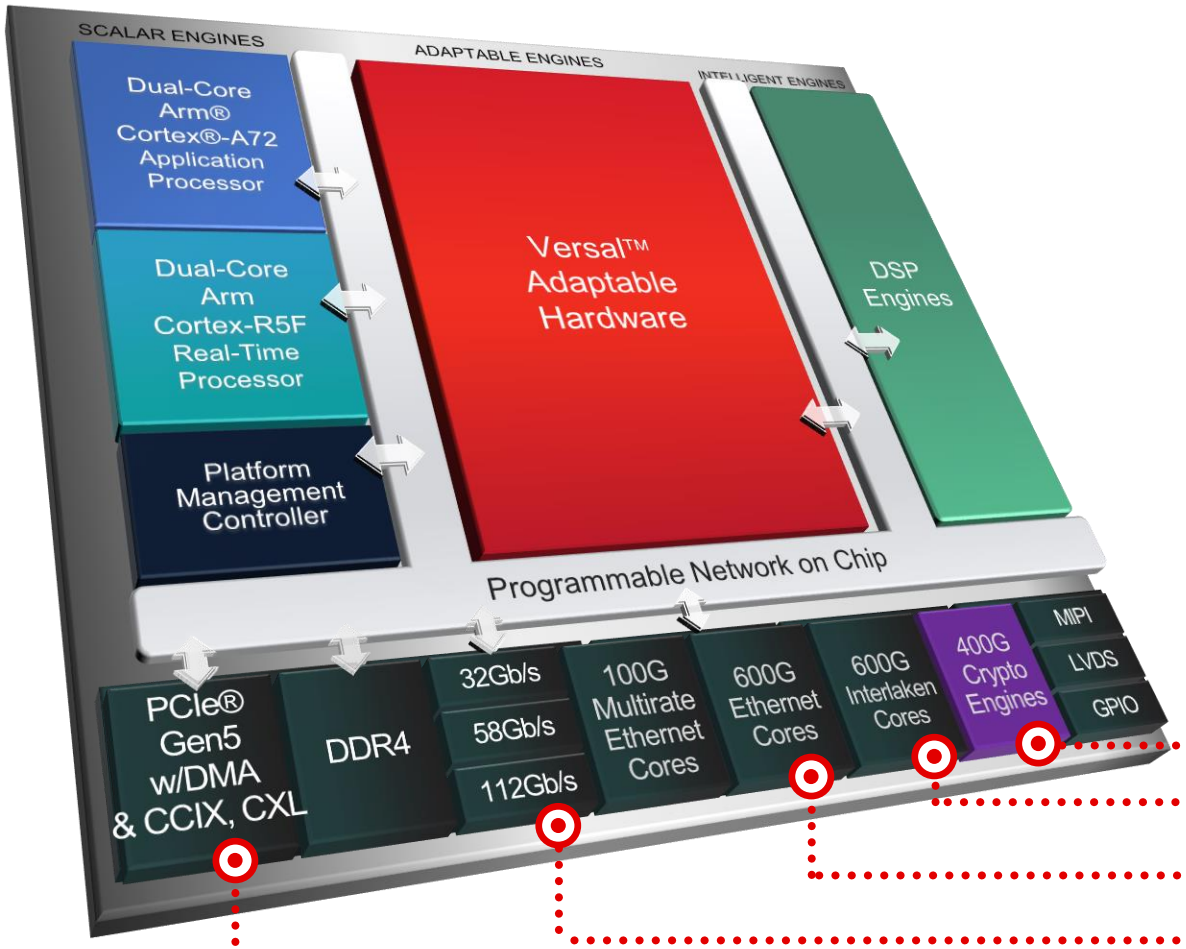
Xilinx – Next Generation Network Security with Versal High Speed Crypto (HSC) & Soft Crypto Engine (SCE) L2 & L3 Protection

Venkat Adusumilli
Strategy and Technical Marketing (Wired & Wireless Group)
vadusumi@xilinx.com

Versal Premium – Interconnected High-Speed Cores



XILINX VERSAL™ | PREMIUM

400G High-Speed Crypto Engines

600G Interlaken Cores

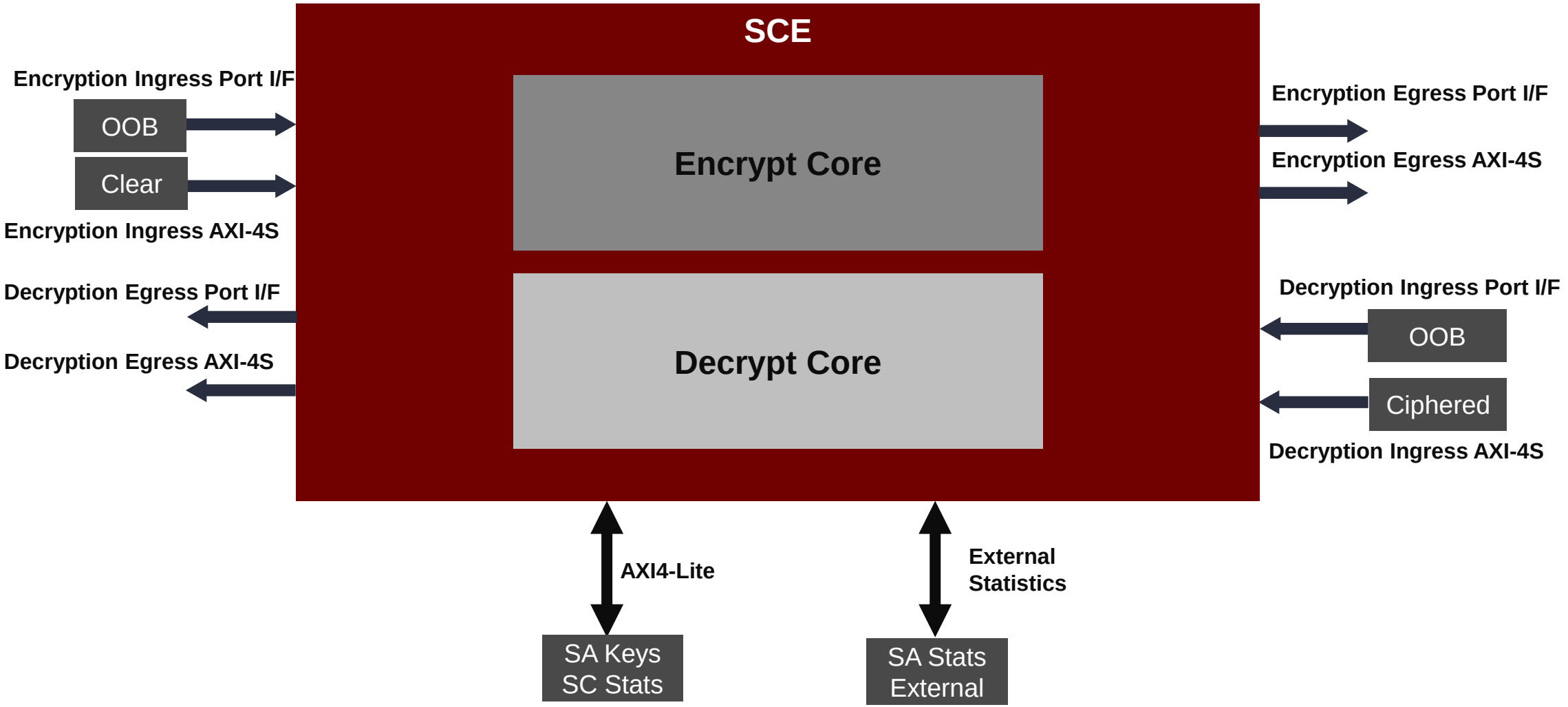
600G Ethernet Cores

112G PAM4 Transceivers

PCIe® Gen5 w/DMA & CCIX, CXL

XILINX

Software Crypto Engine (SCE) Interfaces



XILINX.

SCE - Features

Security Association (SA)

- 512 SAs Supported (Internal Key)
- 1M + SAs with External Memory

Integrity and Confidentiality

- GMAC (I)
- GMAC-AES (I&C)

Cryptography Protocols

- MACSec (0, 30, 50 Confidentiality offsets)
- IPSec
- Bulk Crypto (0-63 Bytes)

Cipher Support

- AES-GCM-128/256
- AES-GCM-XPN-128/256 (IPSec and MACSec only)
- Bulk Crypto

Total Bandwidth

- 200G

Statistics Counters

- 48 Bit Counters

SCE – Features (Cont'd)

Additional Features

- On the Fly Key Expansion
- Internal GHash SubKey Generation
- Replay Protection(Detect Unauthorized Access)
- IPSec Window Size (1-64)
- Bypass Mode (Packets Unchanged)
- 32-bit User Spare information in Encrypt/Decrypt Datapaths
- Key Zeroization
  - Zeroization of Stored Keys
  - Value of "0" as Uninitialized Key
  - CRC32 to validate Key Writes

IPSec Specific

- Setting IV/Salt
  - 32 Bit SALT + 64 Bit IV inserted after ESP header
  - Byte 0 [95:88); Byte 3 [71:64]

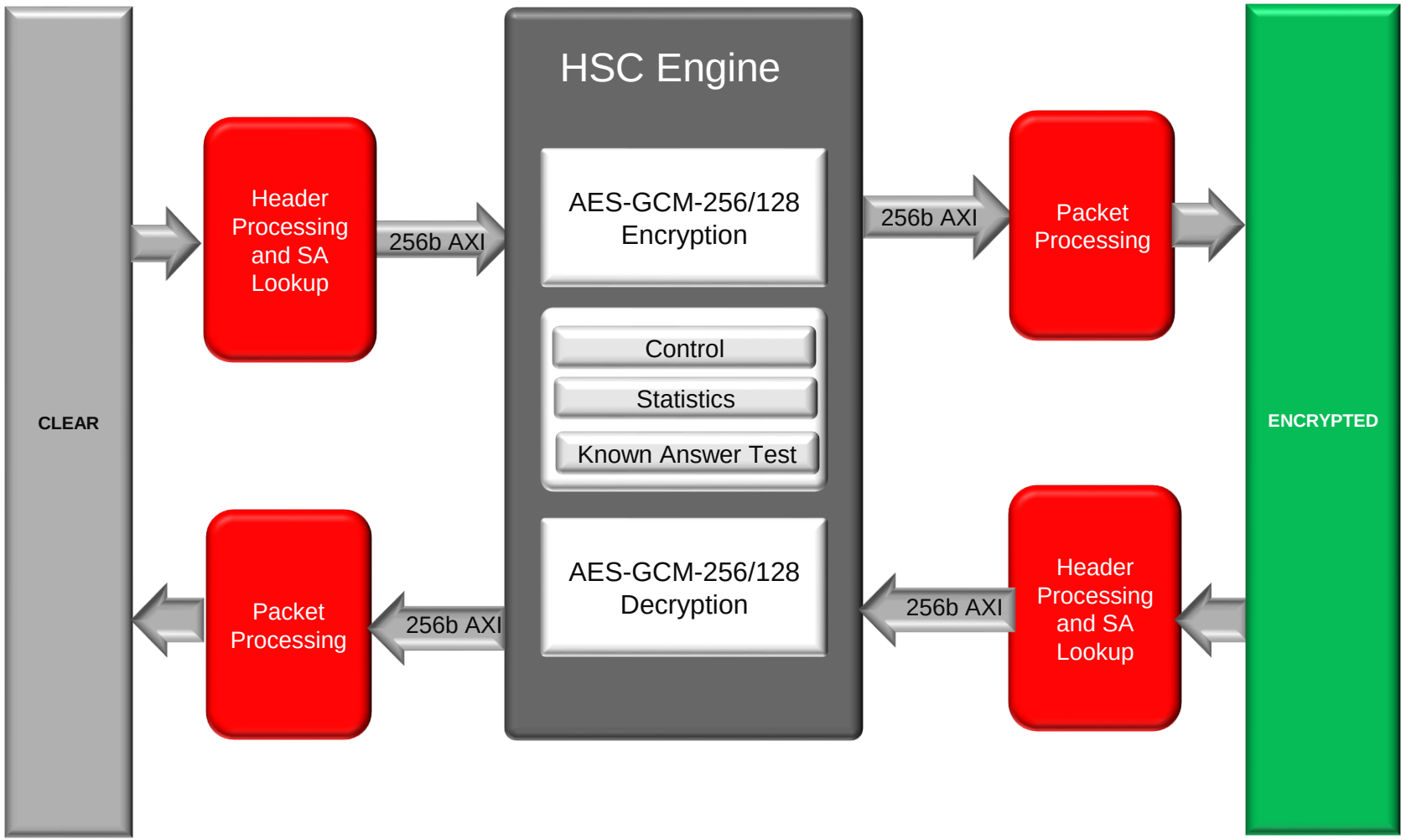
SCE – Configurations & Resource Utilization

Bandwidth	Segmented AXI-S Bus Width	# AXI-S	Frequency (MHz)	Supported Crypto Functionality
40G	128	1	312.5	MACSec, IPSec or Bulk Crypto
50G	256	2	195.3125	MACSec, IPSec or Bulk Crypto
100G	384	3	260.5	MACSec, IPSec or Bulk Crypto
200G	512	4	390.625	MACSec, IPSec or Bulk Crypto

Bandwidth	LUTS	BRAM	Device	Function
200G	223,000 (12%)	186 (7%)	VP1502	IPSec

HSC - Features

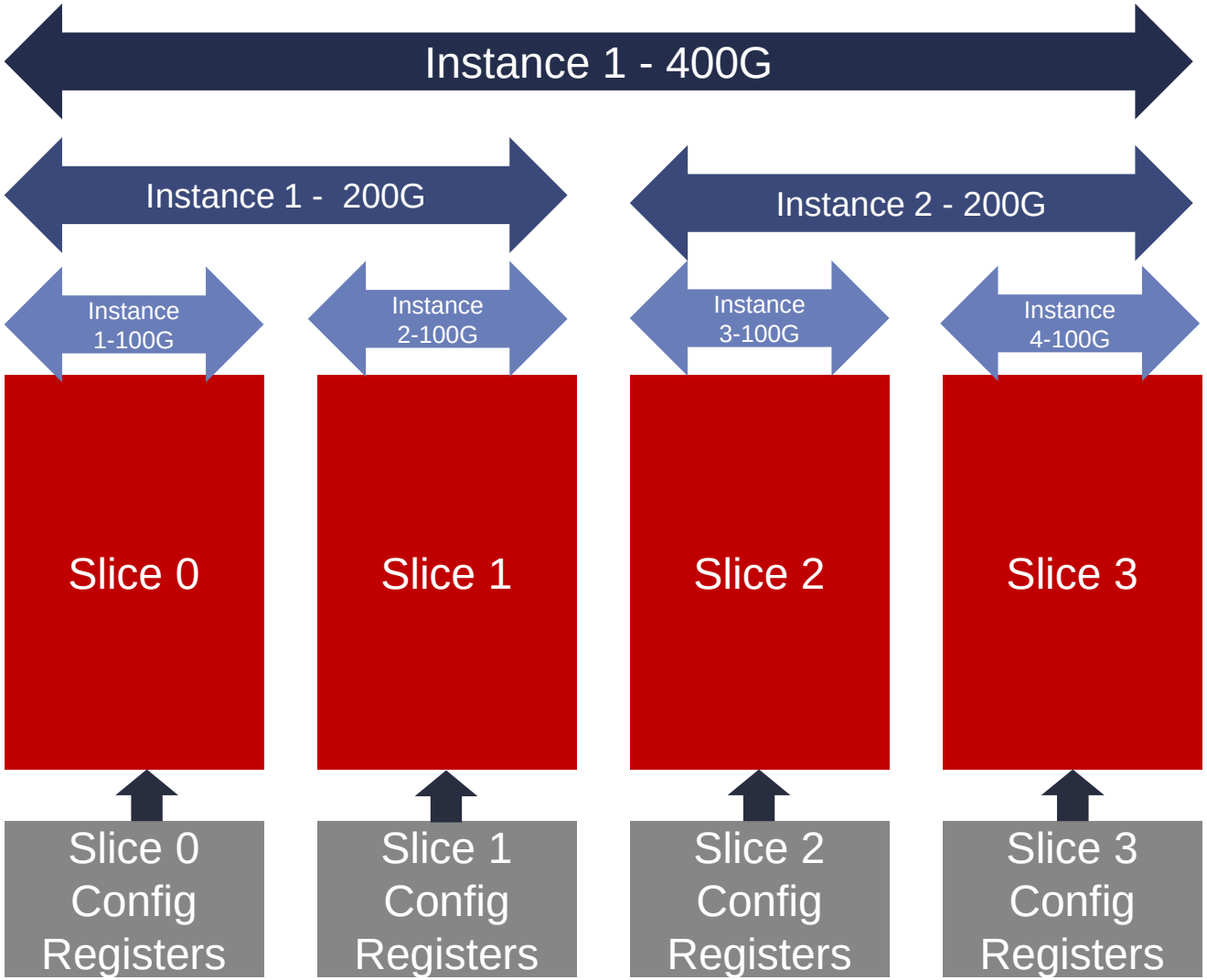
HSC – Block Diagram



- 400G High Speed Crypto Block
  - AES-GCM-256/128 engine
    - 400G of Bulk Encryption
  - 400G of MACSec
    - 4x100G, 2x200G or 1x400G
    - 128 SAs per 100G and beyond
  - 400G of IPSec
    - 4x100G, 2x200G or 1x400G
    - Thousands of SAs with internal and external storage

XILINX.

HSC – Supported Configurations

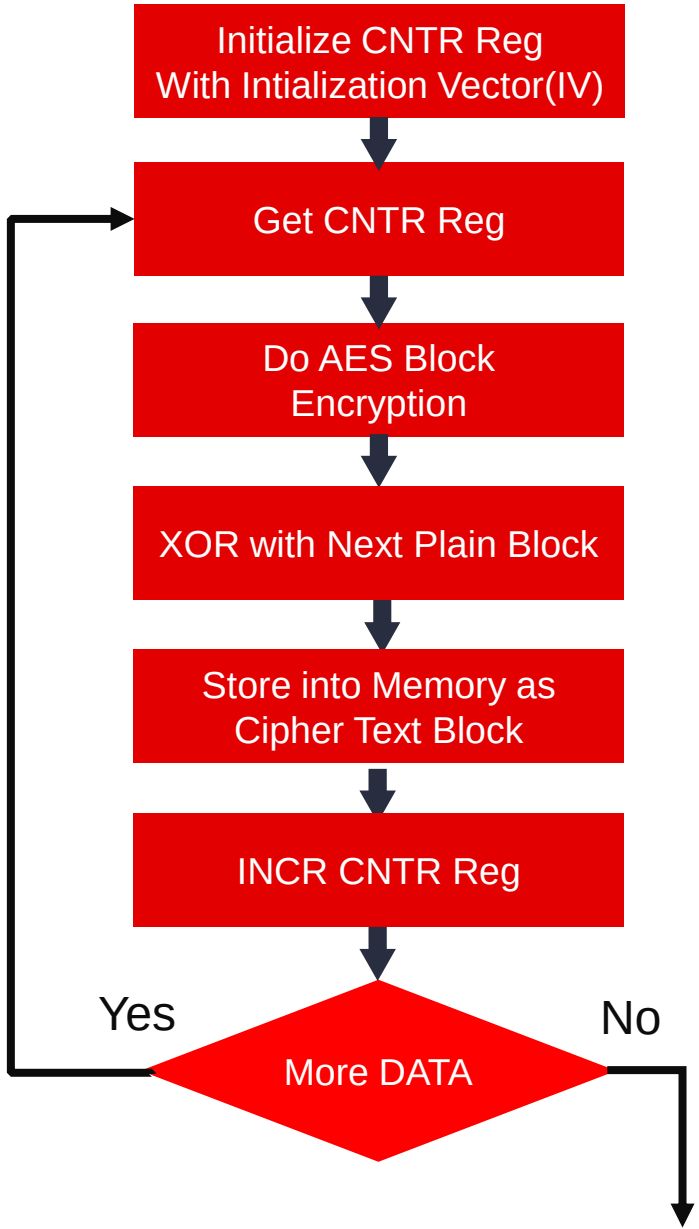


- Modular 100G Slices
- Hardware Programmed Regs
  - Slice Config Vector Register(1bit)
  - Instance Width Register (2 bit)
- Software
  - Hitless dynamic Re-config of Slices within an instance
  - 32 Bit Boundary

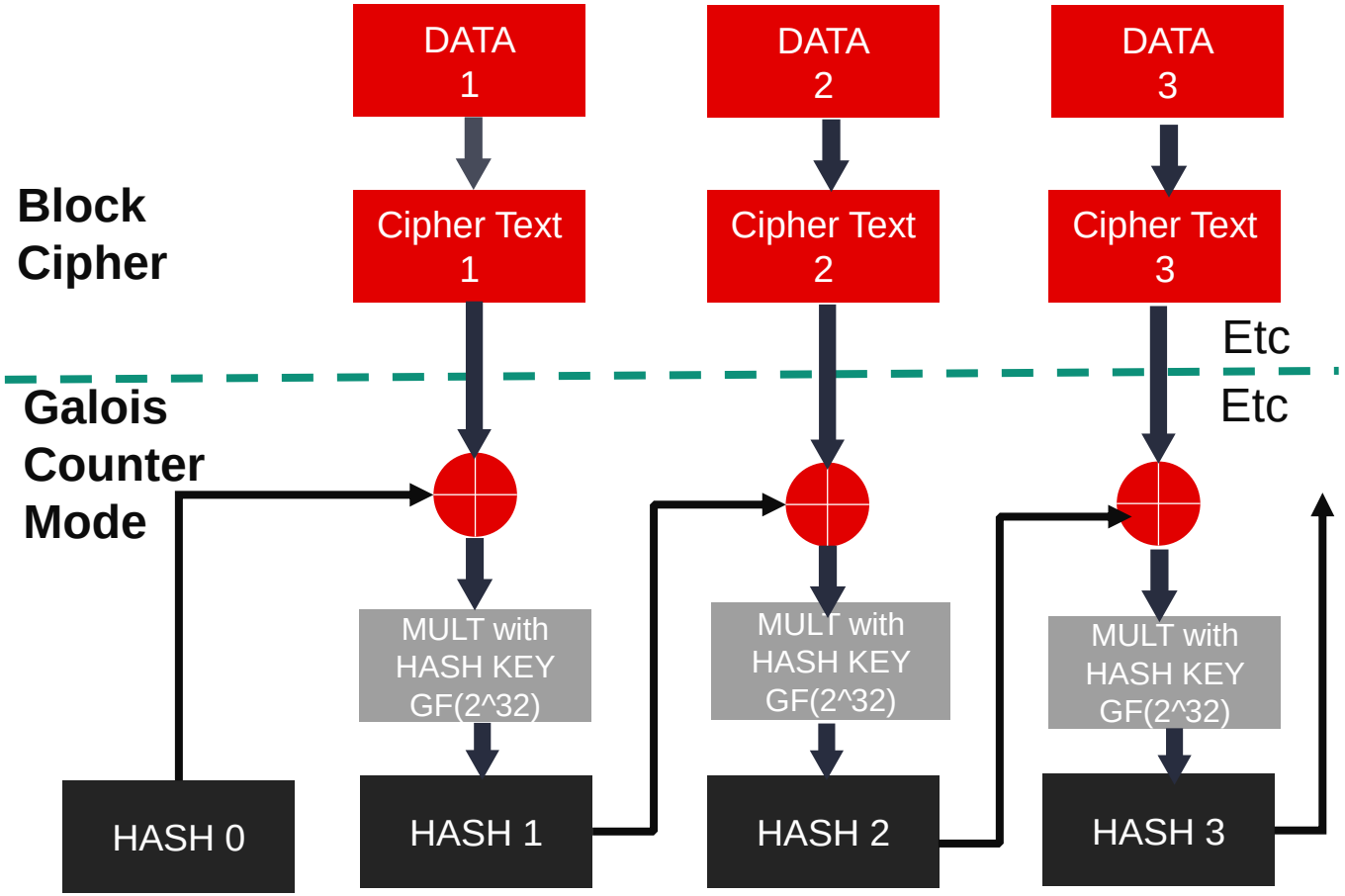
Instances (#)	Bandwidth (Gbps)
4	100
2	200
1	400

XILINX.

AES-GCM-256/128 Algorithm- Auth Encrypted Protocol



FIPS#197
IEEE 802.1ae Standard
RFC- 4106 for IPsec



XILINX.

400G High-Speed Crypto Engines for Secure Networking

Up to 2.0 Tb/s of Encrypted Line Rate Throughput

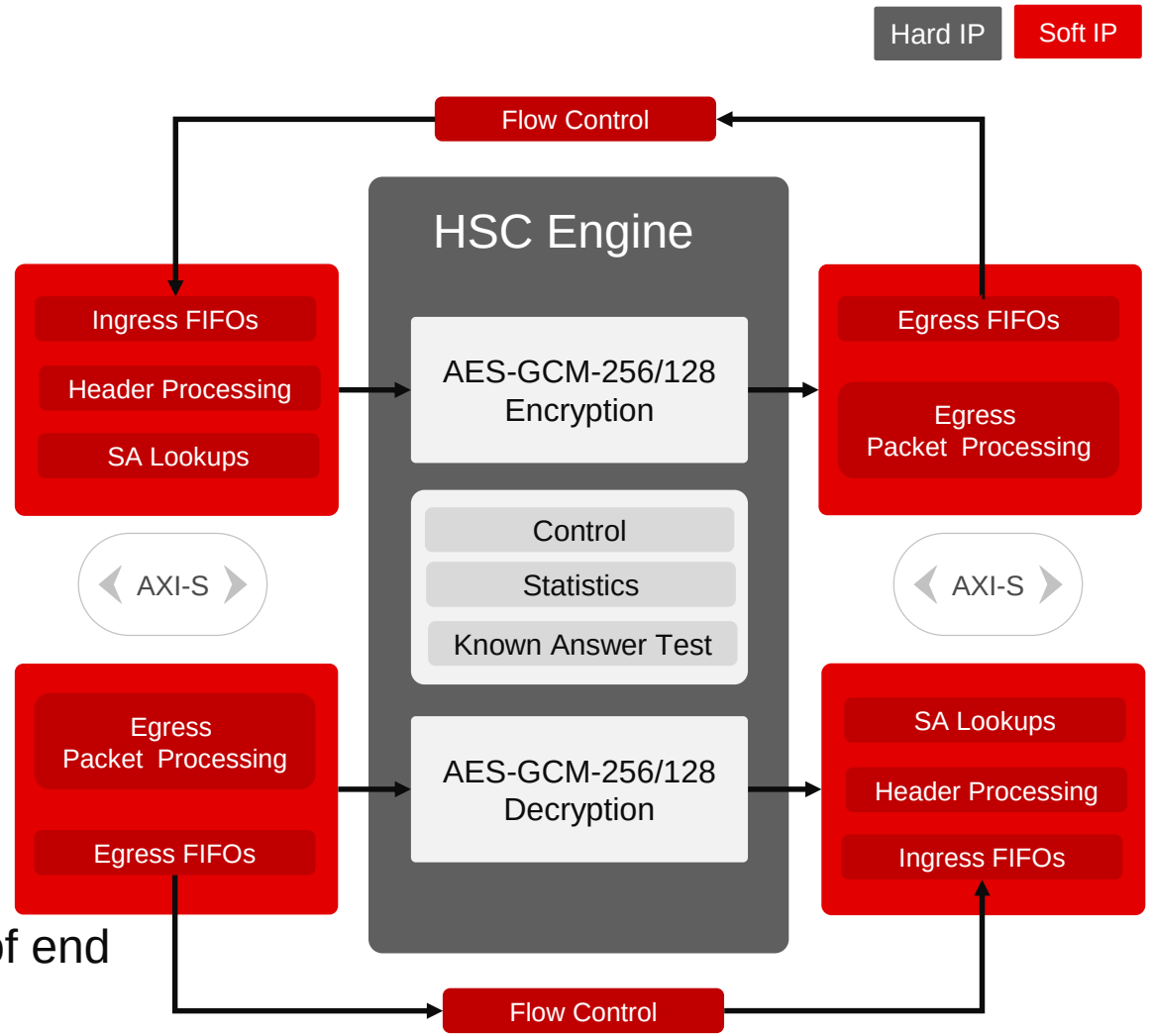
- World's only hardened 400G Crypto Engines in an adaptable platform
- AES-GCM-256/128 engine for encryption/decryption
- Channelized rates: 40x10G to 1x400G
- 128 SAs per 100G, 1M+ SAs with External lookup

MACsec (L2)

- Secures point-to-point or shared Ethernet links
- Simplified, per port Encryption option
- Use cases: LAN, Secure DCI

IPsec (L3)

- Secures connections over IP network
- Flexible, Transport agnostic, and scaling to 1000s of end devices
- Use cases: peer-to-peer VPNs , SSL Decryption, Transport



MACsec Use Model

HSC - Features

Security Association (SA)

- 128 SAs per 100G (Internal Memory)
- 48 bit per SA Statistics and Error Counters
- 512 SA Statistics and Error Counters for Encryption
- 512 SA Statistics and Error Counters for Decryption

Algorithm Validation Support

- 2 Test Modes
- AES AVS
  - Supports KAT(Known Answer Test, MMT(Multi-Block Message Test), MCT(Monte Carlo Test)
- GCM AVS
  - Supports GCM/GMAC Algorithm Validation Suite

Operation

- HSC Interface Frequency 2X Internal Core Frequency
  - Eg: 680 MHz HSC frequency Supports 320 MHz Fabric Frequency

HSC – Features (Cont'd)

- Key Memory
  - Internal Memory to store Keys
  - Key Writes
    - Write Only Access thru Management I/F
  - Key Reads
    - No Reads to Previously Written Keys
  - Key Erase
    - On SOC Power ON
- IPSec
  - Tunnel and Transport
  - ESP(Encapsulating Security Payload)
    - ESP header processing; No IP Header proc
  - Confidentiality, Integrity, Authentication and Replay(SA stored Internal Mem ; 256B Replay protection)
  - IPv4 & IPv6
  - 32b and 64b Sequence# (ESN)

HSC – Features (Cont'd)

- MACSec
  - Secure Channel(100G) Supports SW configurable 64 bit SCI
  - Secure Channel(100G) Supports SecTag (128 bit without SCI or 64 bit with SCI)
    - Sub 100G Channelization (Eg: 10x10G) to be enabled in Soft IP outside of HSC
- Key Management
  - Key Auth, Exchange, Management done external to HSC
  - Keys(All Set to 0's) is available via Control Register
  - Keys written into HSC cannot be Read
    - A Digest of Keys available for Read

HSC - Supported Encryption Ciphers

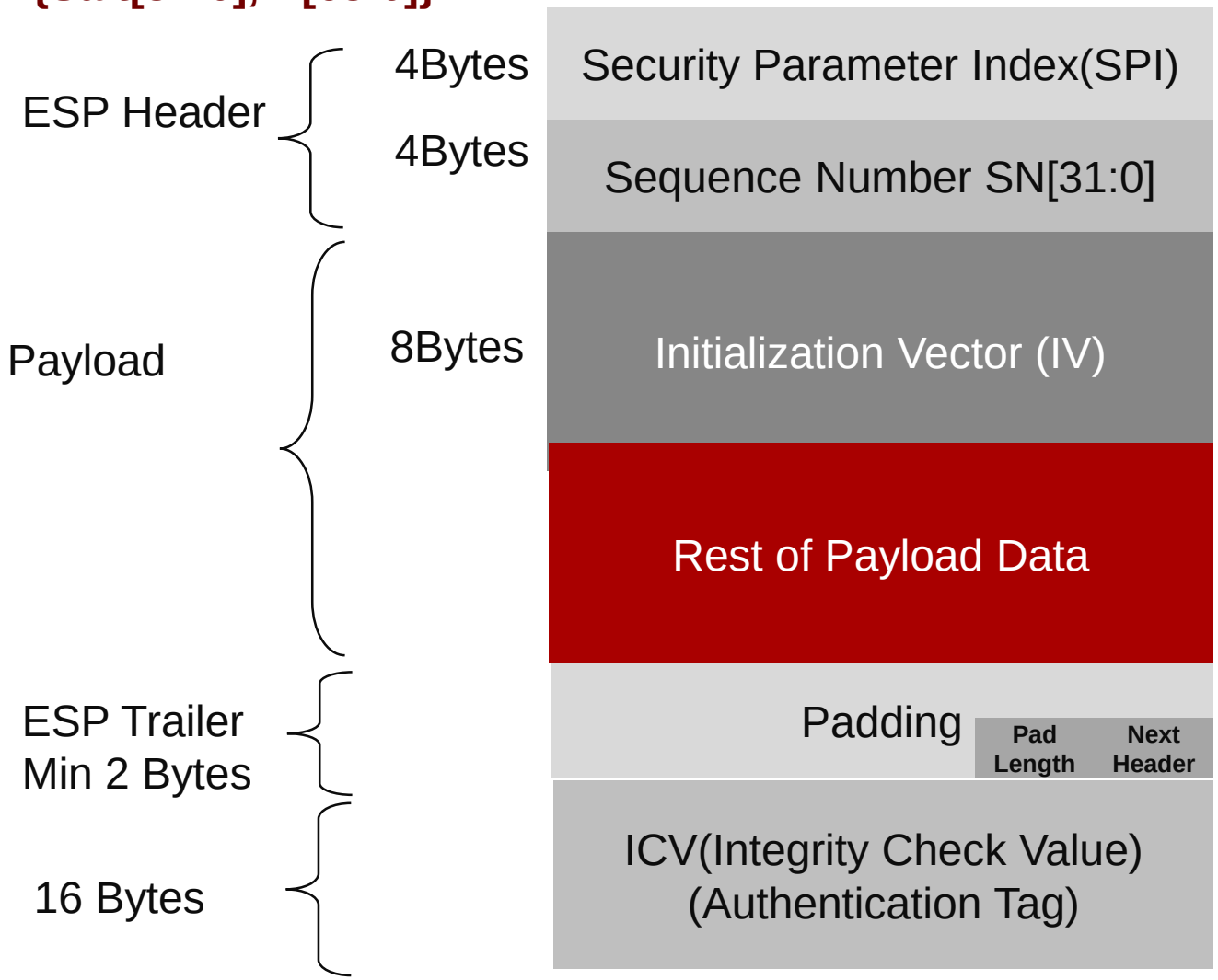
- IPSec
  - AES-GCM-ESP-256
  - AES-GCM-ESP-128
- MACSec
  - AES-GCM-256
  - AES-GCM-128
  - AES-GCM-XPN-128 (Extended Packet Numbering – 64bits)
  - AES-GCM-XPN-256 (Extended Packet Numbering – 64bits)
- Bulk Encryption
  - AES-GCM-256
  - AES-GCM-128

HSC – ESP Packet Format- Encryption with Auth (32 SN)

Plaintext = { Rest Of Payload Data, Padding, PadLength[7:0],Next Header[7:0] }

Nonce = {Salt[31:0],IV[63:0]}

AAD = {SPI[31:0],SN[63:0]}



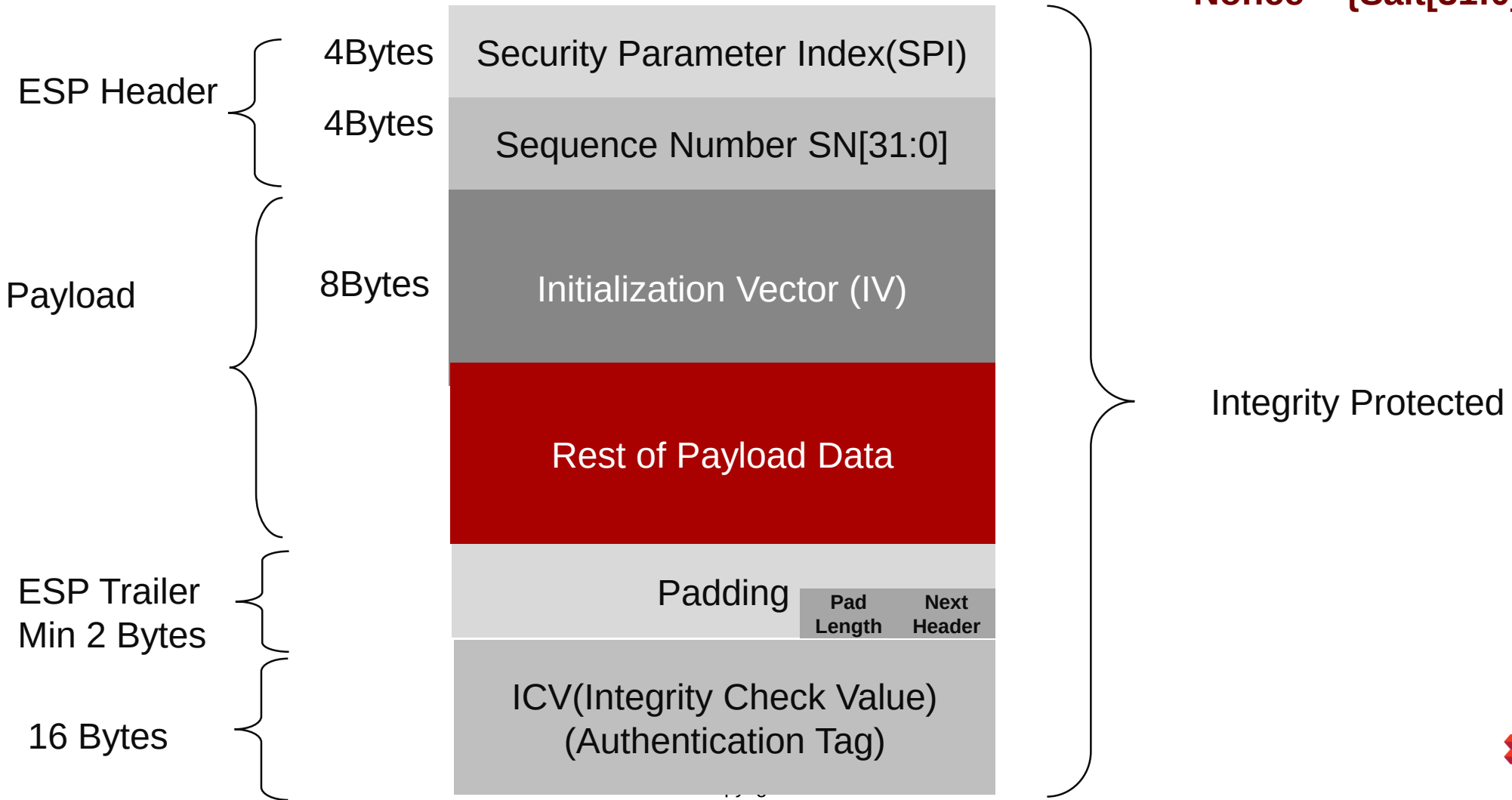
XILINX.

HSC – ESP Packet Format- Authentication Only (32 SN)

AAD = {SPI[31:0], SN[31:0], IV[63:0], Rest Of Payload Data, TFC Padding, Padding, PadLength[7:0], Next Header[7:0]

Plain Text = { }

Nonce = {Salt[31:0],IV[63:0]}



XILINX.

Standards Compliance

IPSec(L3) – Conformance

IPSec Protocol	Conformance
Security Architecture for the Internet Protocol	RFC 4301 (Dec2005)
IP Encapsulating Security Payload	RFC 4303 (Dec 2005)
Cryptographic Algorithm Implementation Requirements and Usage Guidance for Encapsulating Security Payload (ESP) and Authentication Header (AH)	RFC 8221 (Oct 2017)
The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload	RFC 4106 (Jun 2005)
Extended Sequence Number (ESN) Addendum to IPsec Domain of Interpretation (DOI) for Internet Security Association and Key Management Protocol (ISAKMP)	RFC 4304 (Dec 2005)
Advanced Encryption Standard (AES)	FIPS Publication 197 (Nov 2001)
Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC	NIST Special Publication 800-38D (Nov 2007)
Cryptographic Algorithm Validation Program Management Manual, Version 1.0	NIST/CSEC (June 2009)

MACSec(L2) – Conformance Matrix

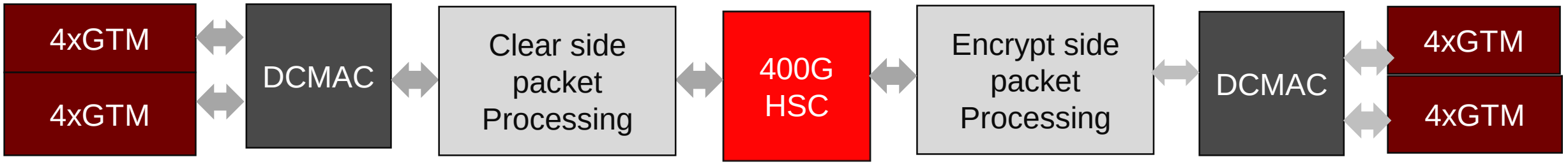
MACsec Protocol	Conformance
Media Access Control (MAC) Security	IEEE 802.1AE (Sep 2018)
Advanced Encryption Standard (AES)	FIPS Publication 197 (Nov 2001)
Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC	NIST Special Publication 800-38D (Nov 2007)

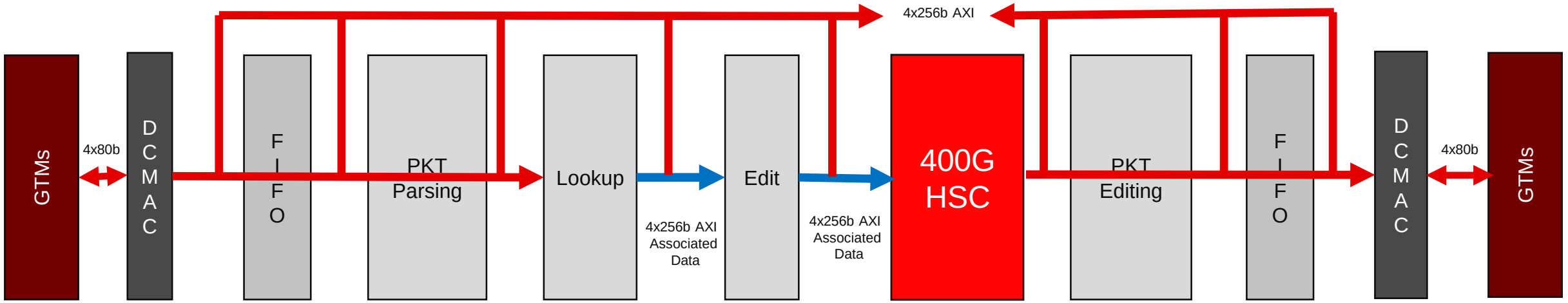
HSC → Versal Premium – Resource Availability

Cores	Versal - Premium
DSP	2000-10000+
NOC	Yes
LUTs	600K-3M+
Distributed RAM	18-103Mb
Block RAM	81-175Mb
URAM	113-724 Mb
APU	Dual ARM cortex A72
RPU	2 Arm Cortex R5
PCIe	Gen4 and Gen5
MRMAC	2-8
600G MAC/FlexE	1-7
600G Interlaken	1-3
HSC- 400G (AES-GCM-256/128)	1-5

Use Cases

400G HSC - MACSec/IPSec → Packet Processing





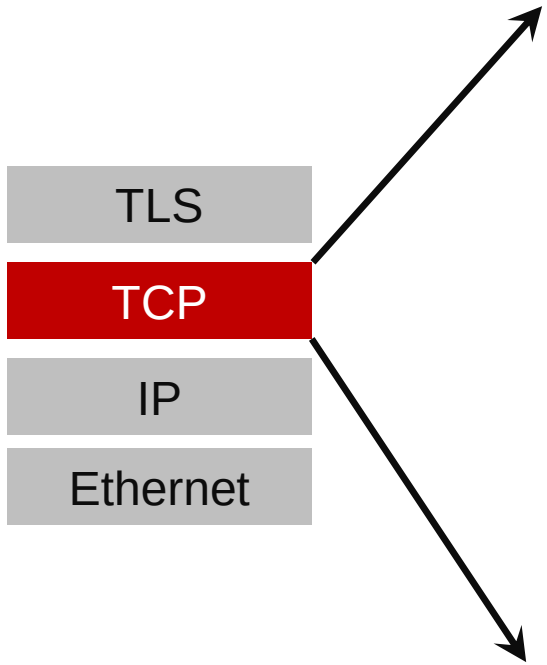
XILINX.

HSC → Versal Premium – Resource Availability

Cores	Versal - Premium
DSP	2000-10000+
NOC	Yes
LUTs	600K-3M+
Distributed RAM	18-103Mb
Block RAM	81-175Mb
URAM	113-724 Mb
APU	Dual ARM cortex A72
RPU	2 Arm Cortex R5
PCIe	Gen4 and Gen5
MRMAC	2-8
600G MAC/FlexE	1-7
600G Interlaken	1-3
HSC- 400G (AES-GCM-256/128)	1-5

TOE IP – TCP Processing – Layer 4

TCP Offload Engine (TOE) Requirements (IETF RFCs)

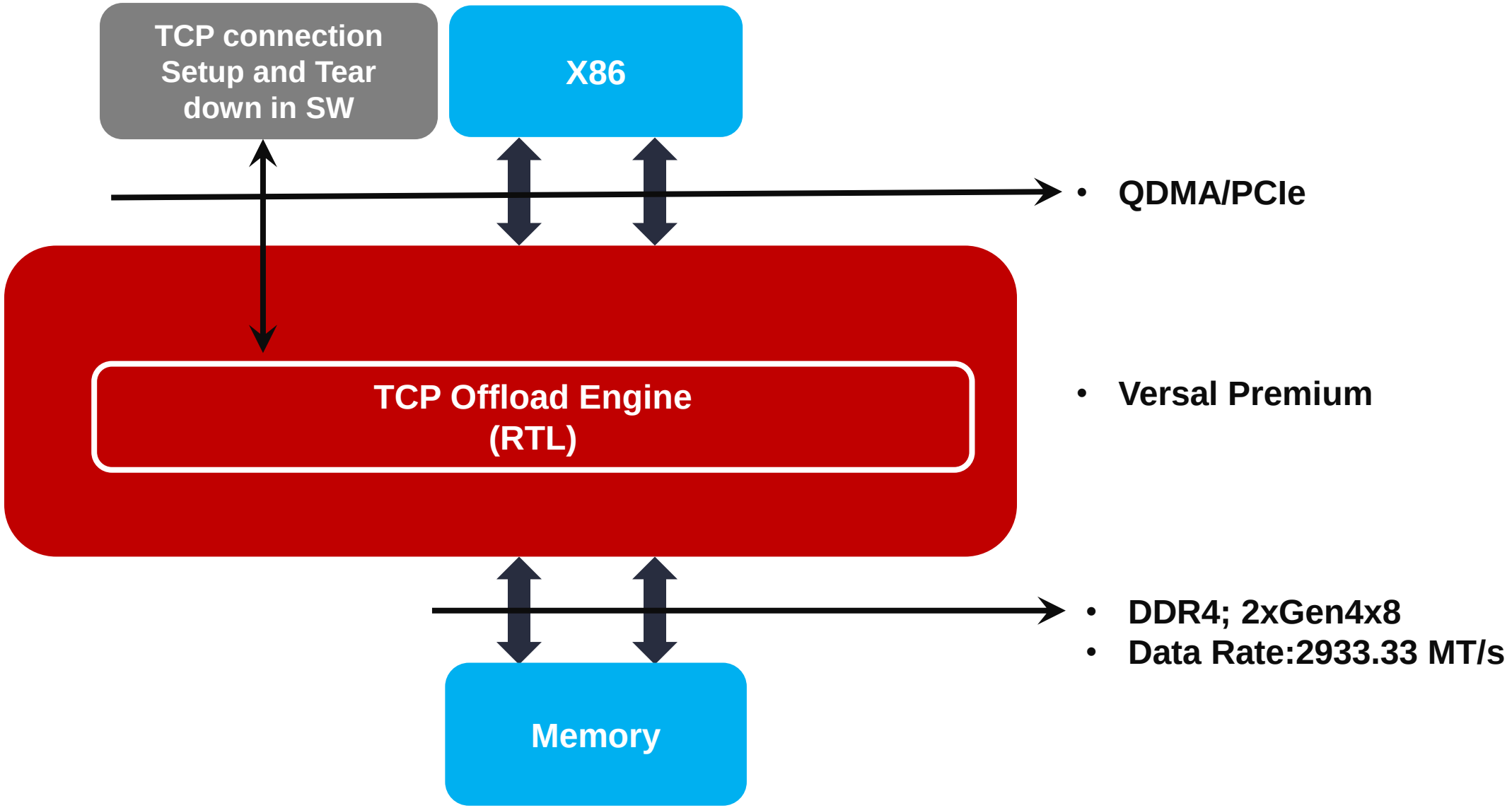


Requirements (IETF Request for Comment Technical Specifications)
RFC 793 TCP Protocol [1981]
RFC 1122 Delayed ACK [1989]
RFC 2018 Selective ACK [1996]
RFC 3168 Explicit Congestion Notification [2001]
RFC 4861 Neighbor Discovery for IPv6 [2007]
RFC 2581/5681 TCP Congestion Control [2009]
RFC 6298 Computing Retransmission Timers [2011]
RFC 8312 CUBIC Congestion Control, BIC
RFC 6582 New Reno [2012]
RFC 1323/7323 TCP Extensions for High Performance [2014]

TCP Security Requirements
RFC 2385 TCP MD5 signature for BGP -Supported
TCP Sequence Number Randomization (ISN) (ISN is done in Software)
TCP Syn Cookies; BBR Algoirthm
Additional Requirements
Search Lookup: • 512-bit RX Search Lookup • 4K bit Session Entry
Timers
• Supported

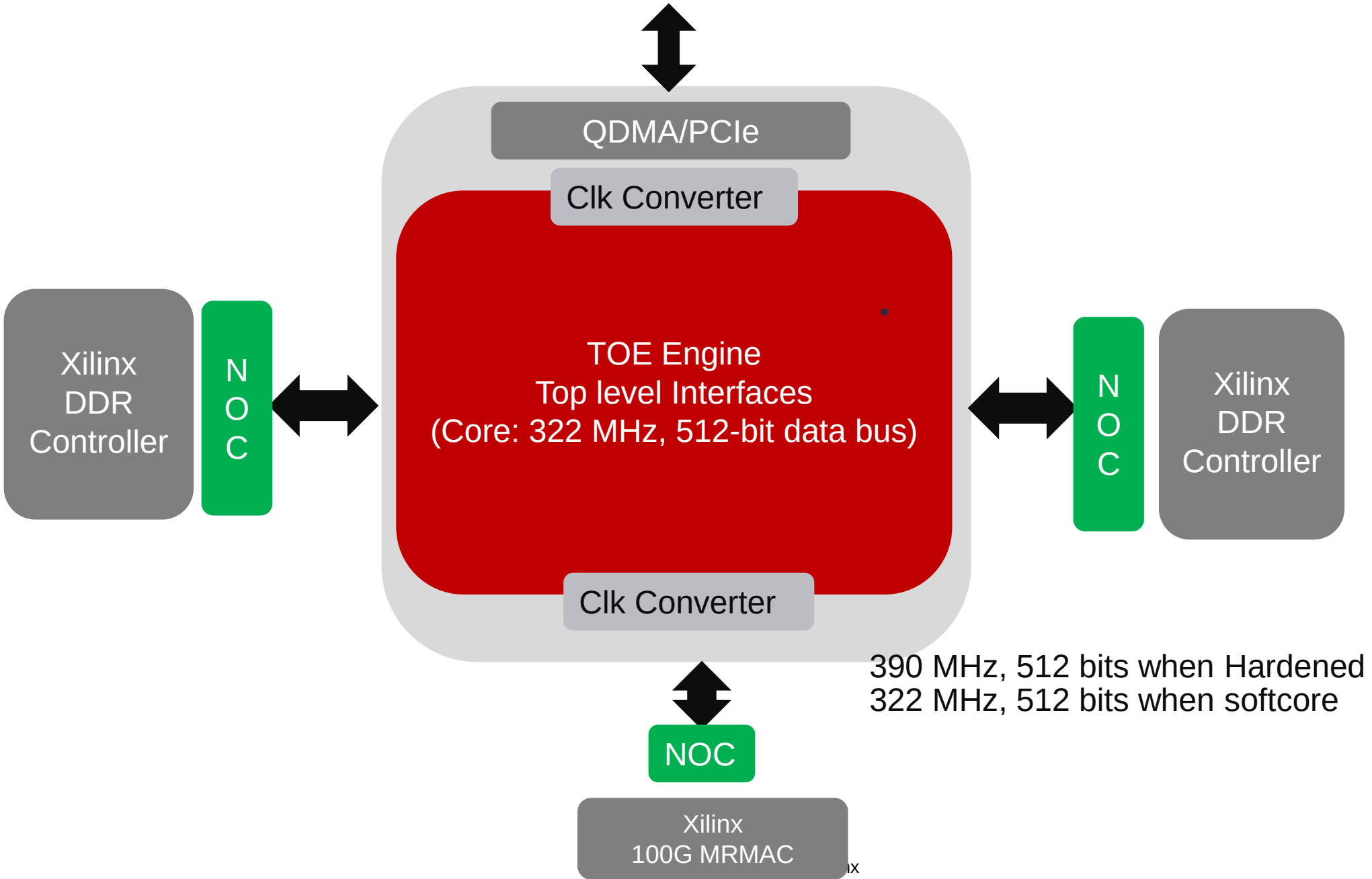
XILINX.

TOE FPGA Interfaces



XILINX.

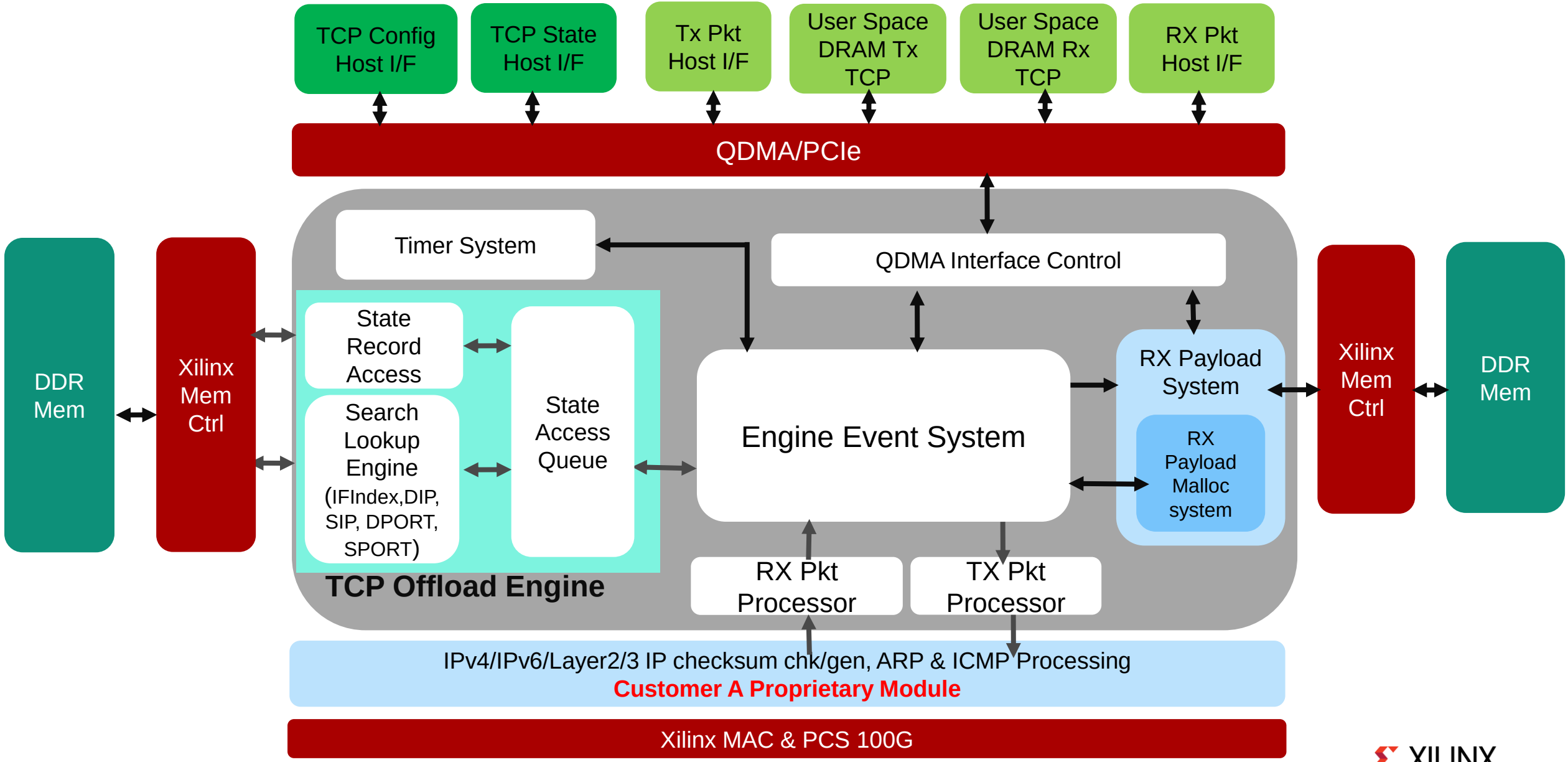
TOE Entity Signal Interface → QDMA/PCIe



390 MHz, 512 bits when Hardened
322 MHz, 512 bits when softcore

XILINX.

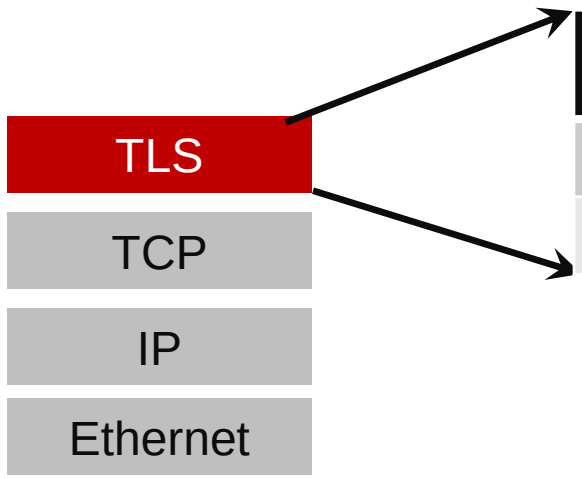
TOE IP - FPGA Architecture



XILINX.

Application Security Offerings : TLS 1.3

TLS Offload Engine (TLSoE) Requirements (IETF RFCs)



Requirements (IETF Request for Comment Technical Specifications)
RFC 8446 TLS 1.3
RFC 5246 TLS 1.2

Symmetric Crypto

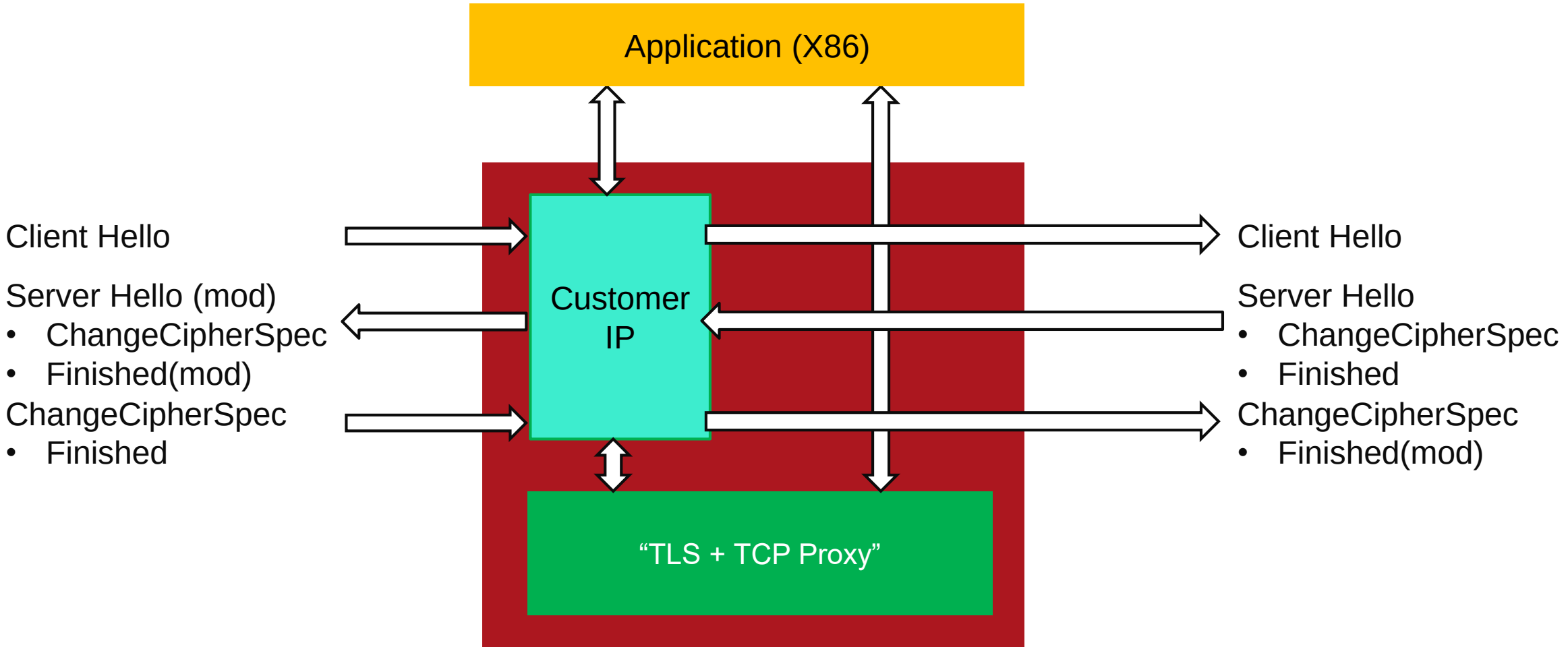
Cipher
- Chacha20Poly1305
- AES-GCM-128/256

Assymetric Crypto(PKI)

- ECC based
- ECDSA, ECDHE

XILINX.

“TLS1.3 + TOE” High Level View

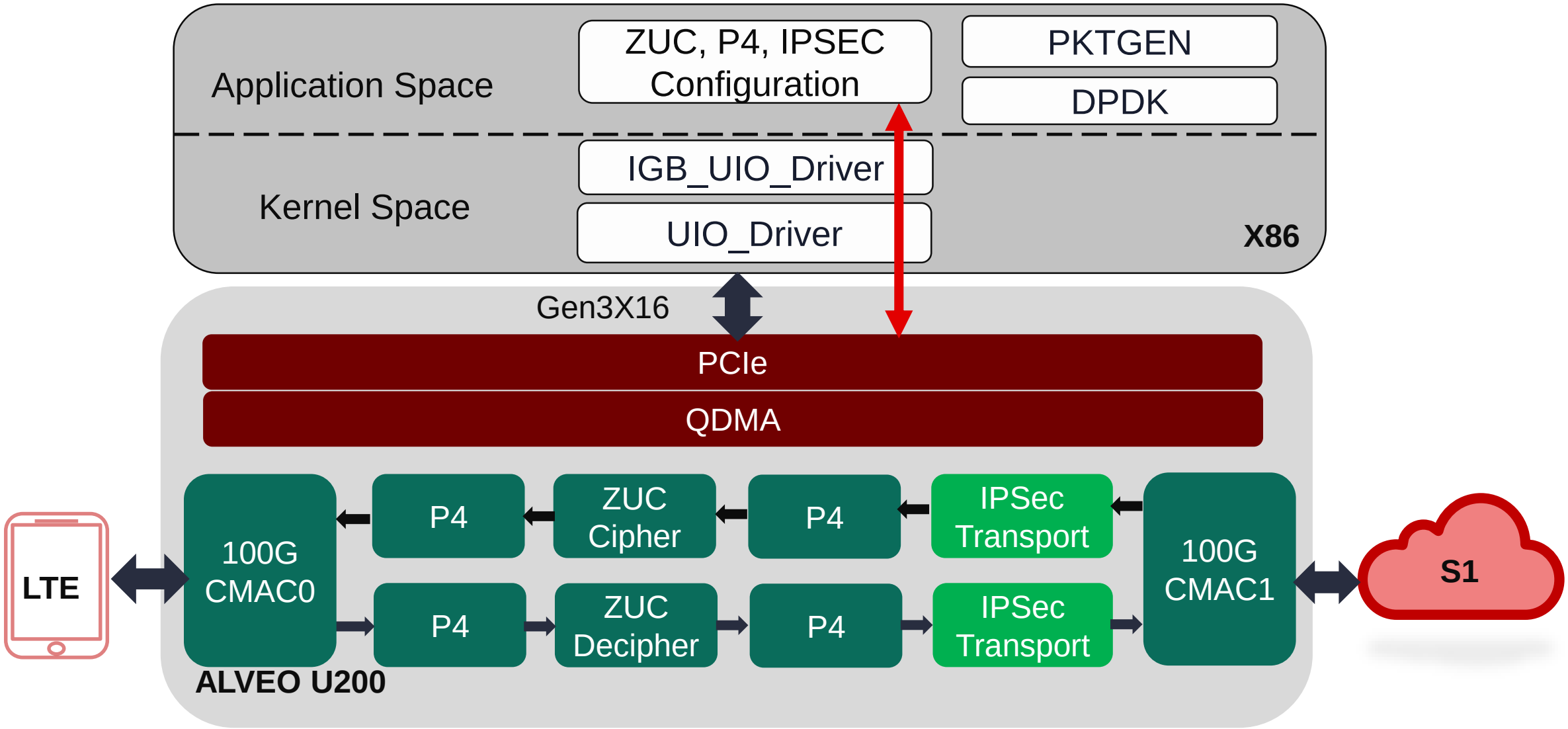


XILINX.

XILINX

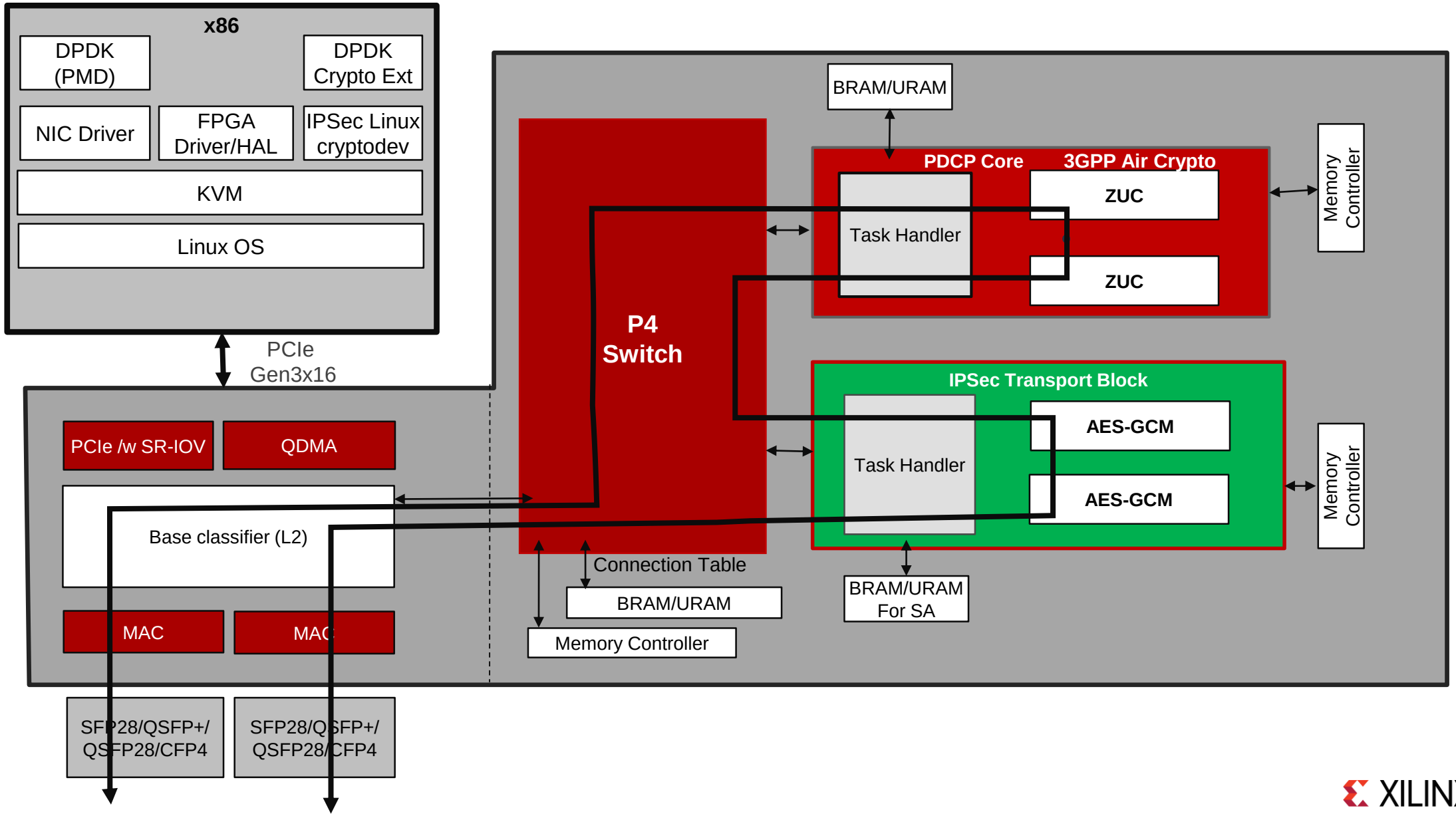
Wireless Application
5G RAN Security (IPSec)

vRAN Split Option 2 (PDCP) – System Architecture



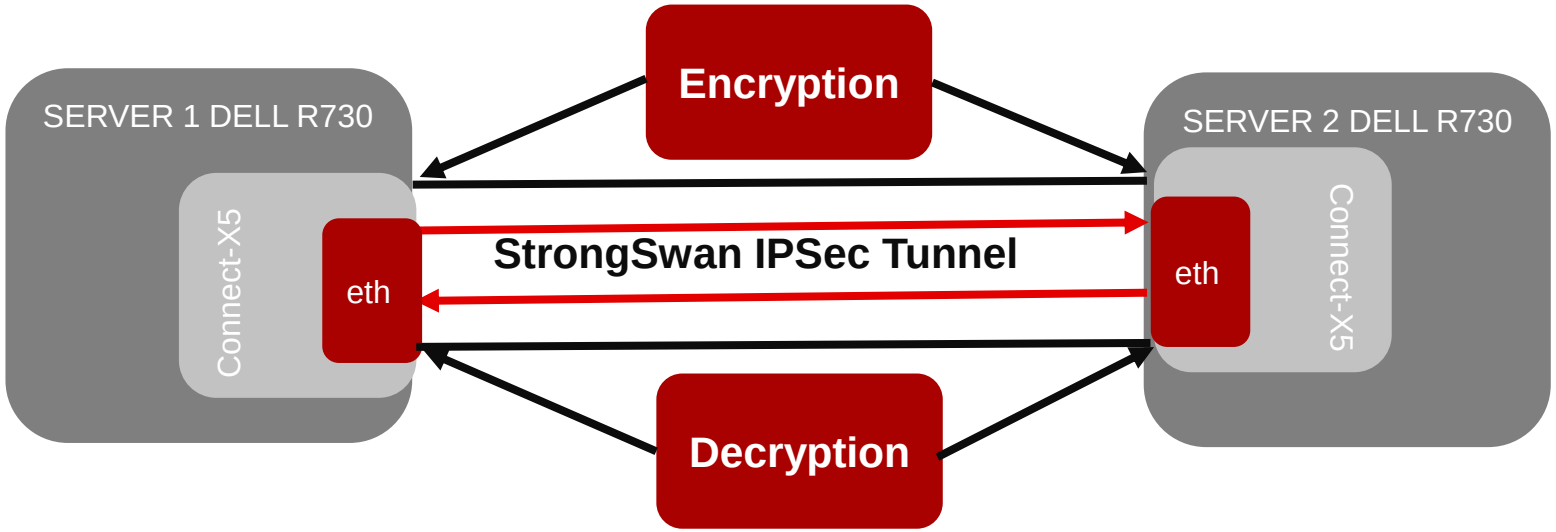
XILINX.

RAN Acceleration – PDCP & IPSec



IPSec Latency Benchmark – SW Vs FPGA

PKT Size	128B	256B	512B	1024B	1514B
Latency (FPGA) uS	1.930	2.030	2.216	2.600	2.960
Latency (SW) uS	160	190	195	205	215

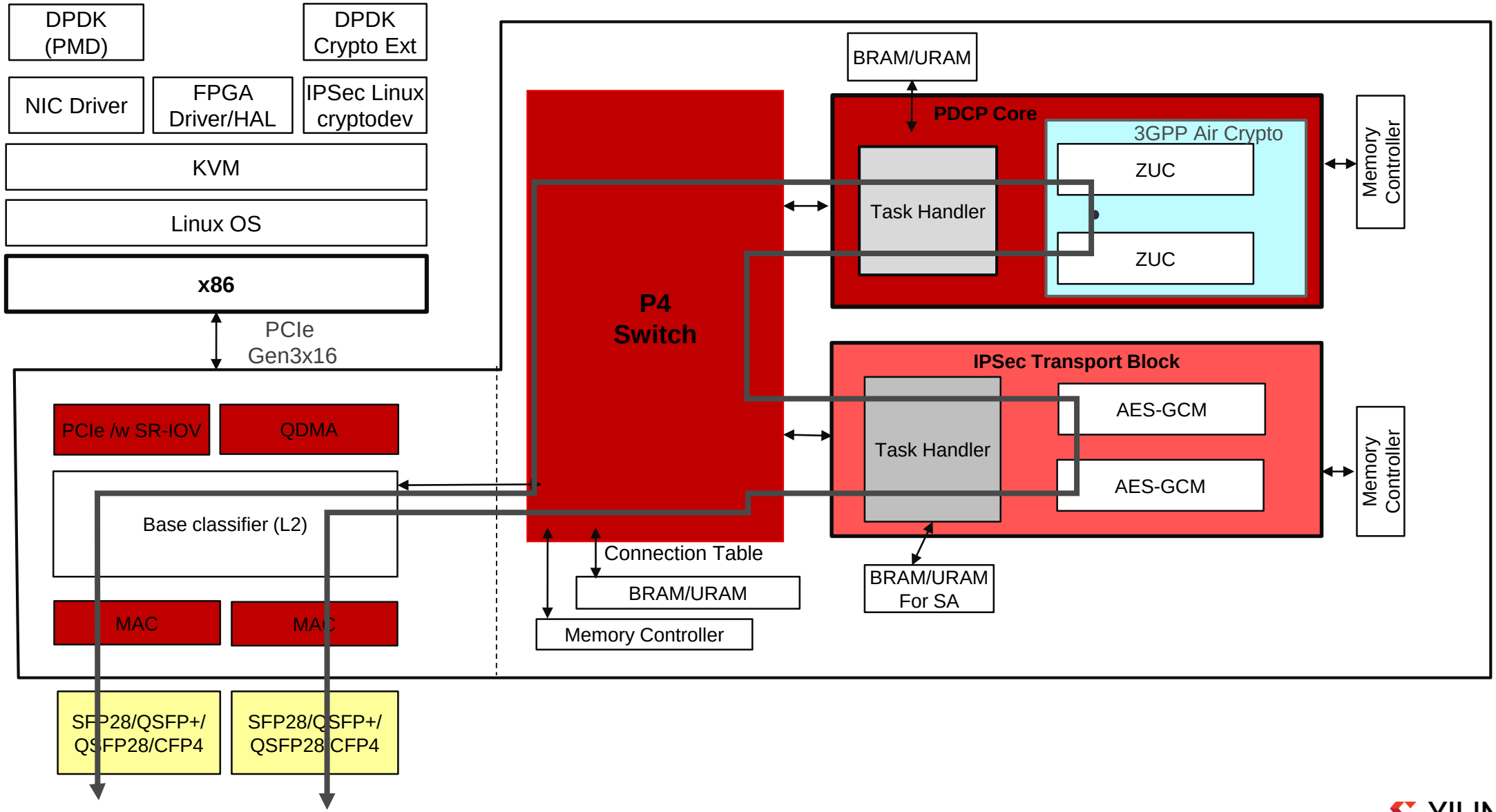


ISAKMP - Key Exchange
AES-GCM-256
Encrypt/Decrypt
Latency- Socket Appl
Client/Server

Perf - iPerf

XILINX.

PDCP →In-Line Design



XILINX.

Thank You