Crypto – Security – IPSec

Hemant Agrawal (NXP)
Akhil Goyal (NXP)

DPDK Summit - India- 2019

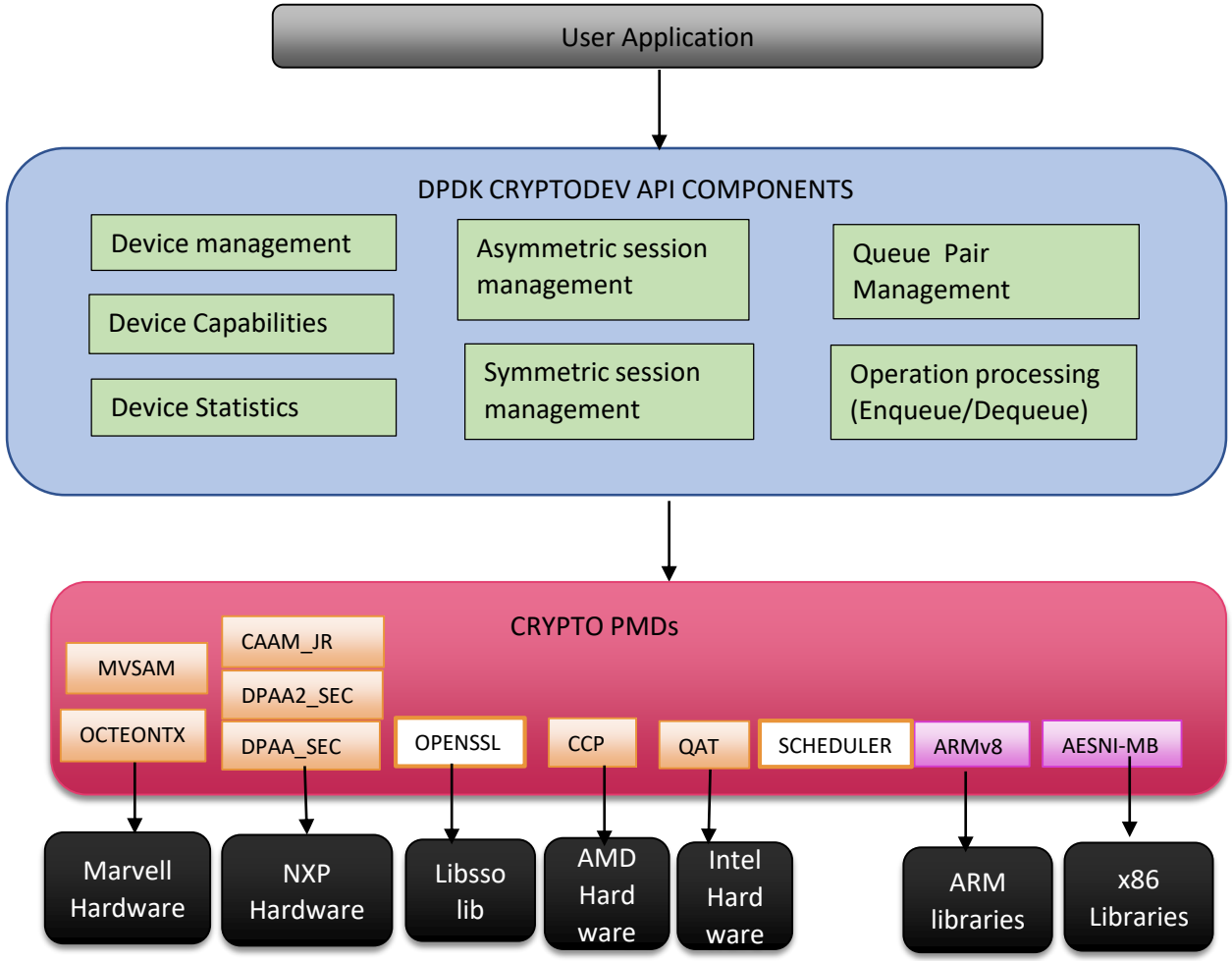
DPDK
DATA PLANE DEVELOPMENT KIT

Agenda

- Cryptodev
- Security
  - Acceleration enablement modes
    - Lookaside Security Protocol
    - Inline Crypto
    - Inline Security Protocol
- IPsec library
- Event Crypto Adapter
- Sample Application
- Future Work
- Q&A

CRYPTODEV

- A framework for processing symmetric and asymmetric crypto workload.
- Provides a standard API supporting transparent crypto processing for all vendors of crypto(SW/HW) PMD.
- Poll mode driver infrastructure with the recent addition of event mode support.
- User can choose to use any combination of software/hardware PMD and schedule work between them

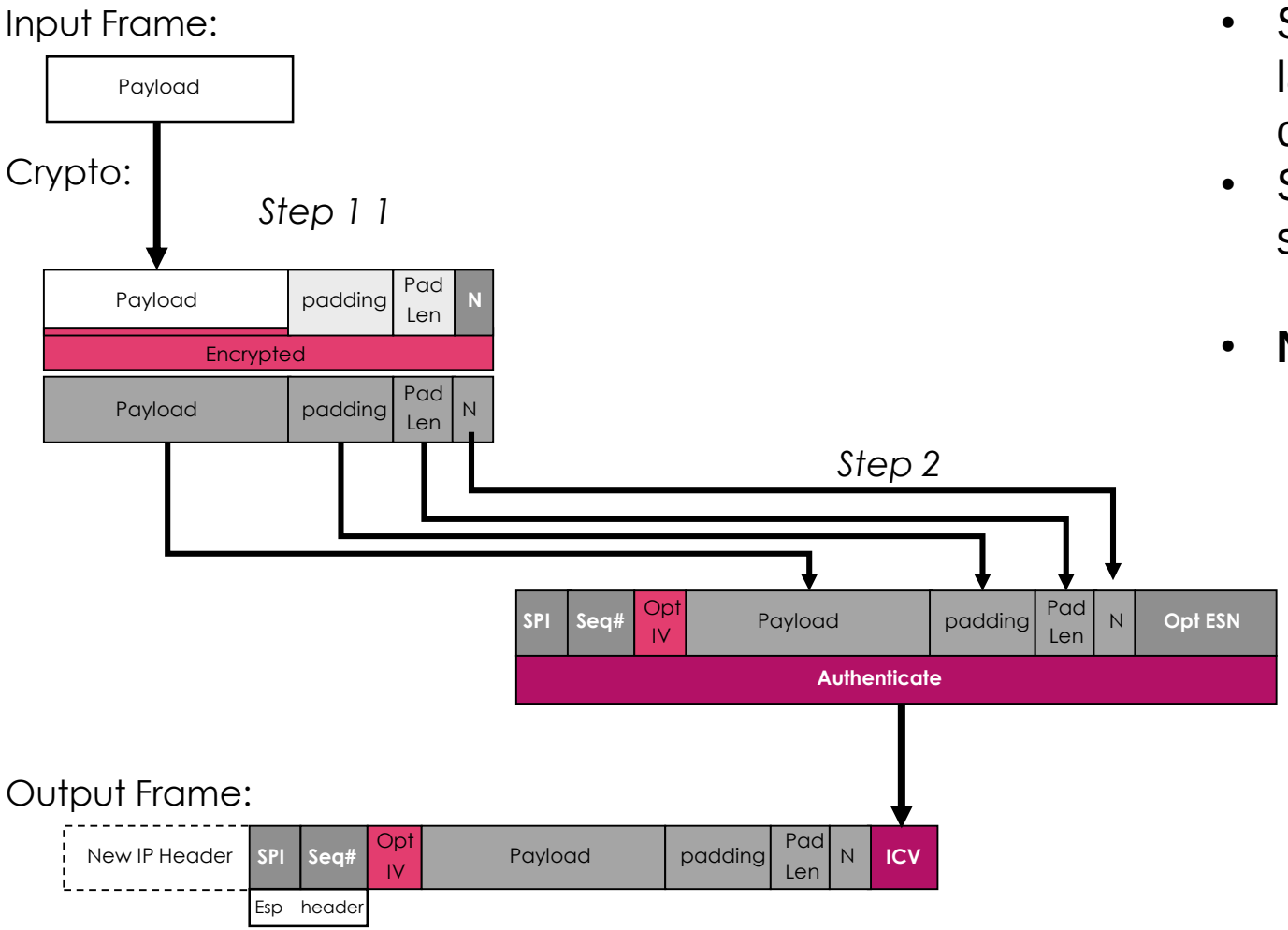


DPDK Crypto Subsystem

- Session-less Mode
  - For each job, software defines;
    - The data to be operated upon (input buffers, lengths, offsets)
    - The output buffers to hold results
    - The cryptographic operations to be performed
    - Keys & context for the cryptographic operations
- Session Oriented Mode
  - For each job, software defines;
    - The data to be operated upon (input buffers, lengths, offsets)
    - The output buffers to hold results
  - Cryptographic operations, keys & context are defined at session establishment time, and referenced for each job
- Operations
  - Symmetric Crypto operations including chaining
  - Asymmetric Crypto operations
  - Hardware off-load processing
- Supports virtual and physical crypto devices
  - Virtual Device (Software Implementation)
    - Intel AES-NI/vector operations, or ARM NEON instructions
    - Open SSL
  - Physical Device (Hardware Accelerated)
    - NXP DPAA-SEC, Marvell's OCTEONTX or Intel QAT
- Test Applications
  - L2fwd with crypto
  - ipsec forward application
  - Test crypto performance


DPDK
DATA PLANE DEVELOPMENT KIT
RTE_SECURITY

Protocol Processing Example - IPsec ESP Tunnel Encrypt

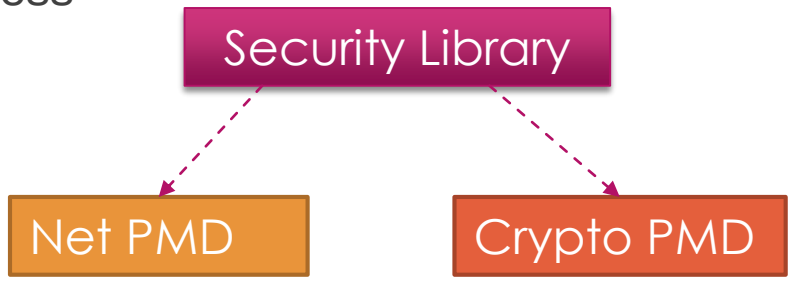


- Security protocol processing like IPsec has a large processing overhead in terms of CPU cycle cost.
- Security HW accelerations can offload it and offer substantial performance + cycle cost savings.

- **NXP Lookaside Protocol Accelerator adds**
  - **ESP header**
  - **Initialization Vector (IV)**
  - **ESP trailer**
  - **Integrity check value (ICV)**
  - **Outer IP header/NAT-T header**
  - **Calculates IP header length**
  - **Calculate header checksum.**

DPDK Security Offload - RTE_SECURITY

- Framework for management and provisioning of hardware acceleration of security protocols.
- Generic APIs to manage security sessions.
- Net/Crypto device PMD initializes a security context which is used to access security operations on that particular device.
- Rich capabilities discovery APIs
- Currently PDCP & IP Security (IPsec) protocol offloads are supported.
- Could support a wide variety of protocols/applications
  - Enterprise/SMB VPNs — IPsec
  - Wireless backhaul — IPsec, PDCP
  - Data-center — SSL
  - WLAN backhaul — CAPWAP/DTLS
  - Control-plane options for above — PKCS, RNG



Security Acceleration Types

DPDK
DATA PLANE DEVELOPMENT KIT

Simple Crypto Lookaside

- Packet enqueued to SW/HW PMD for crypto processing and dequeued to host after processing is complete.
- No protocol headers are modified by the driver

Lookaside protocol offload:

- Packet enqueued to accelerator for processing and dequeued to host after processing is complete.
- All protocol related processing is done by the hardware accelerator

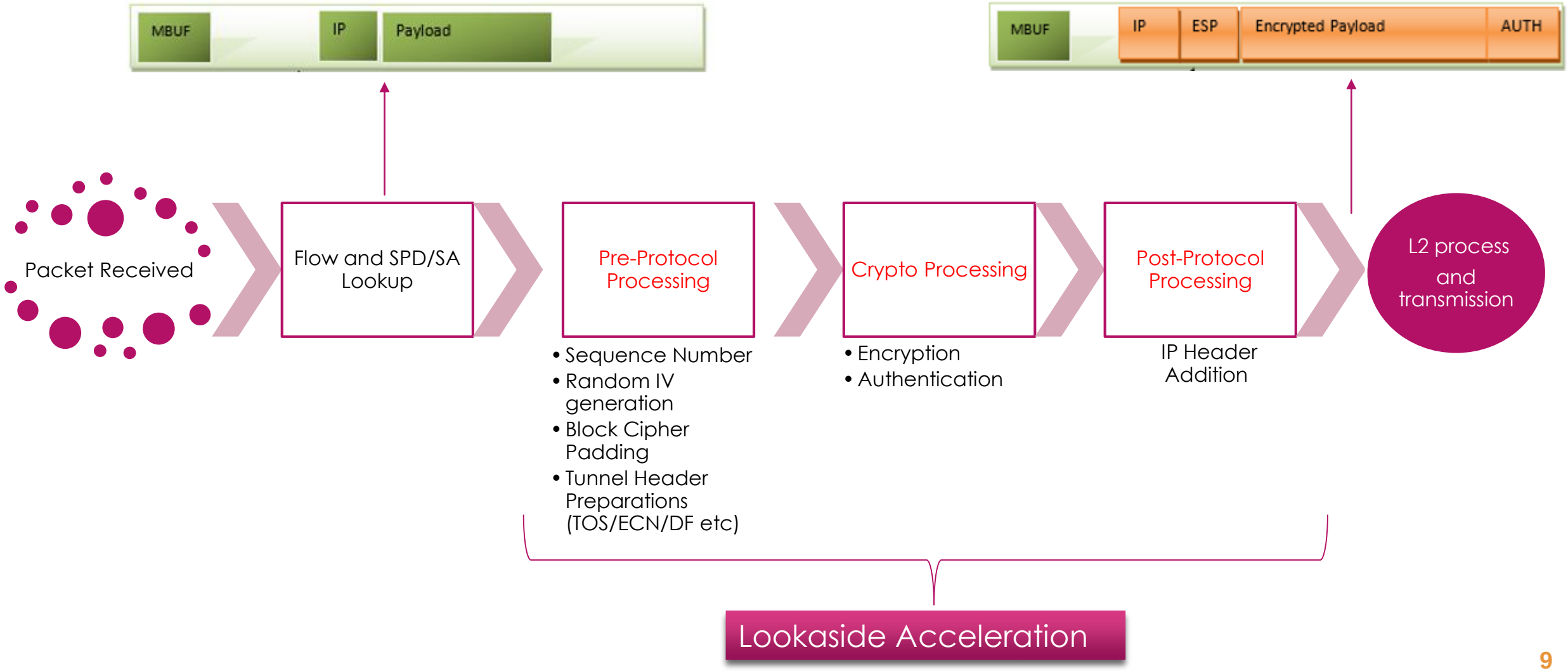
Inline Crypto

- Acceleration is performed on the NIC interface as the packet is ingresses/egresses.
- No protocol headers are modified

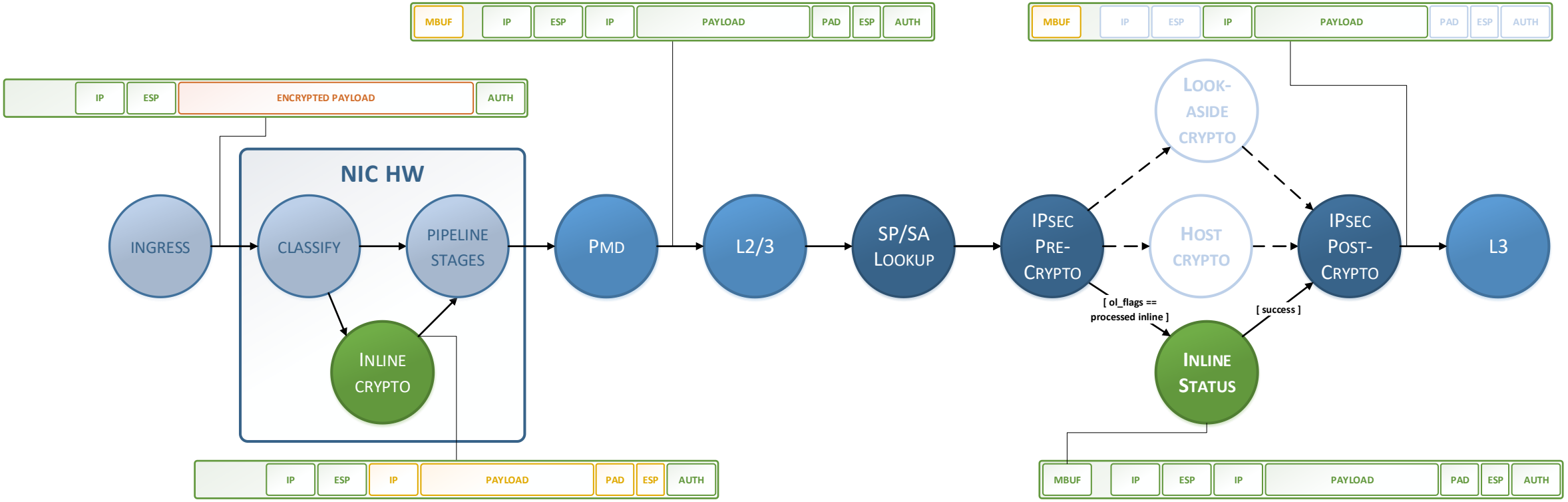
Inline Protocol

- Acceleration is performed on the NIC interface along with protocol processing.
- Protocol headers are also updated by the hardware.

IPSEC - Encrypt Packet Processing



Inline Crypto Ingress Data Path



- NIC HW will decrypt and authenticate the packet on matching (SIP, DIP, ESP)* - mark the result in metadata
- PMD provides the following info per packet:
  - Crypto result – success/failure.
  - Inner ESP next protocol*
  - Packet without a trailer*
- Application:
  - Check mbuf->ol_flags for PKT_RX_SEC_OFFLOAD / PKT_RX_SEC_OFFLOAD_FAILED
  - Read the inner ESP next protocol to remove the ESP header

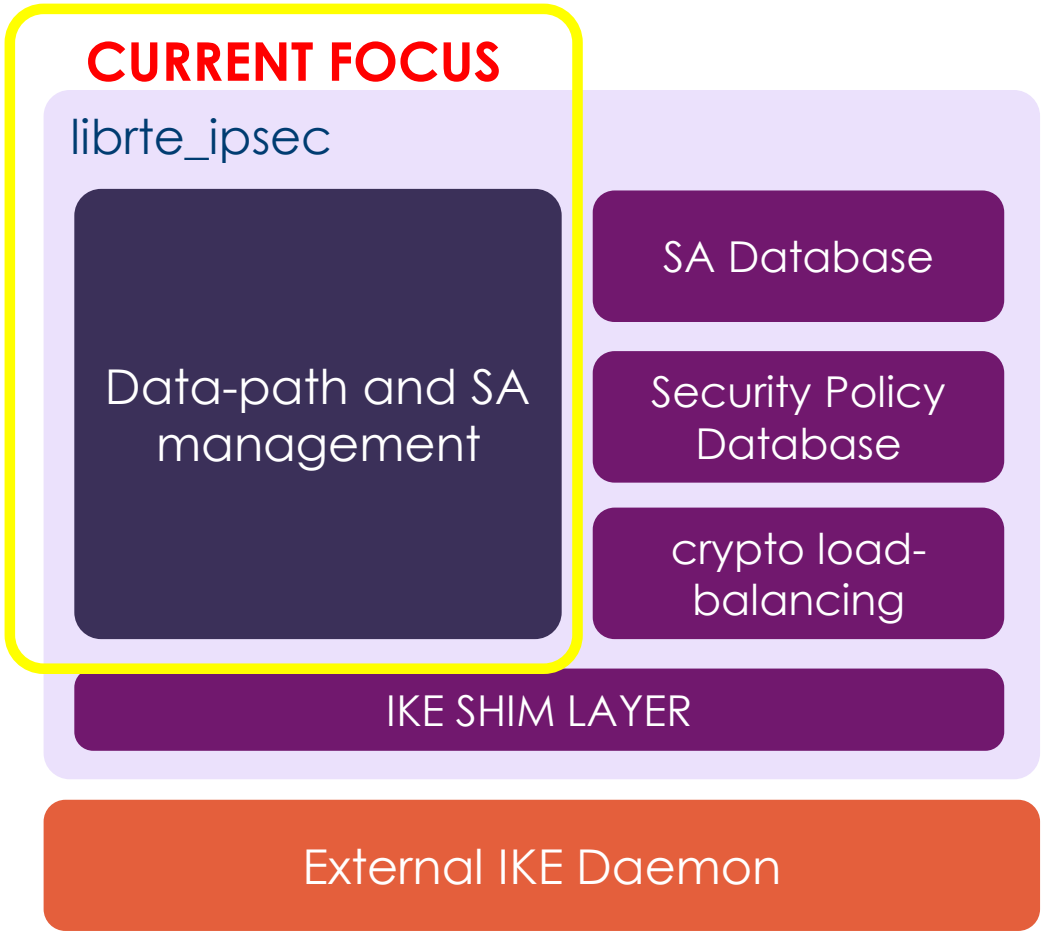
Inline Protocol Acceleration

- IO based acceleration performed on the physical interface as the packet ingresses/egresses the platform.
- Interface performs all crypto processing for the security protocol (e.g. IPsec) during transmission and reception.
- **Packet headers modification is performed on hardware** including all state management and encryption/decryption and authentication operations.
  - Hardware may support extra features like padding of payload etc.
- **Application can retrieve the SA information stored in the userdata on the ingress side to identify the SA for which the packet is decrypted**.
- Requires that ARP entries for MAC headers are programmed along with the security action, as host may not know destination IP in case of a tunnel mode SA

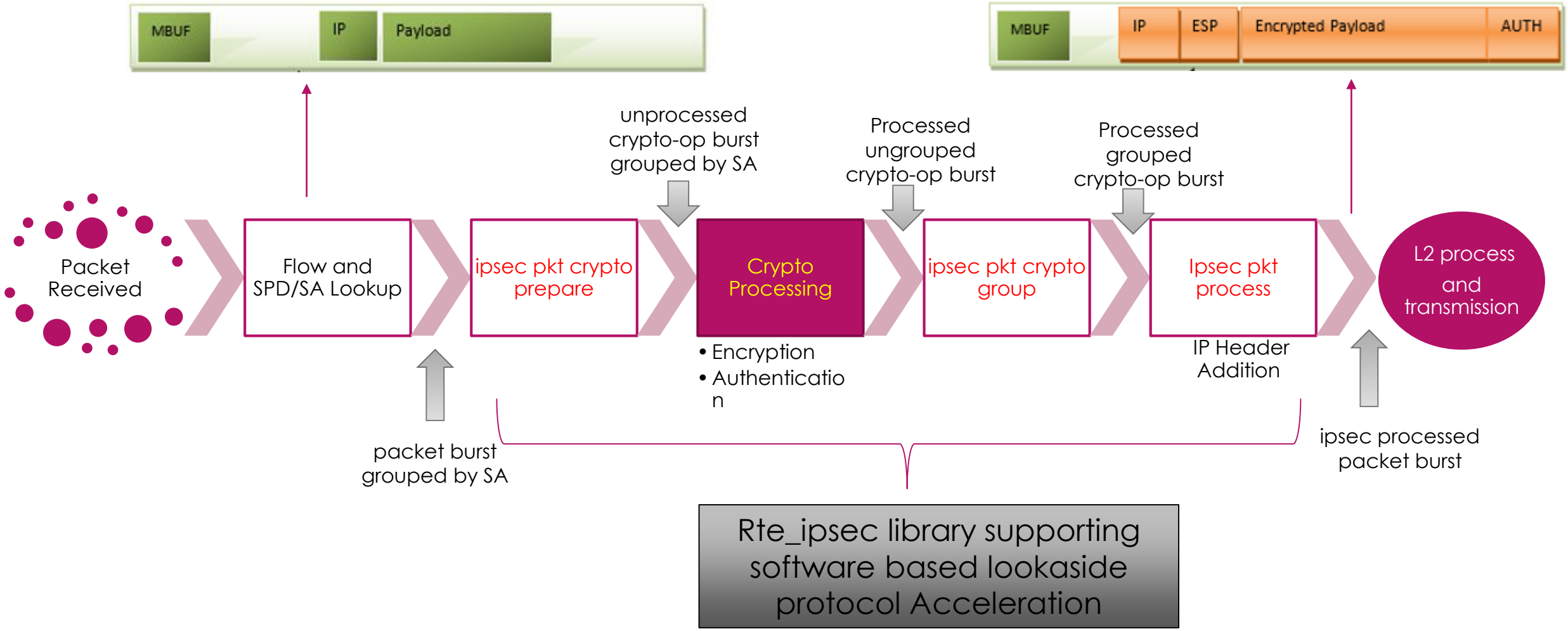
RTE_IPSEC LIBRARY

rte_ipsec library

- A library to provide a generic IPSEC protocol functionality for both data path as well as control path(SA management)
- Basically with the help of IPSEC library, application code would be similar for both protocol offload as well as non-protocol data paths.
- It can be scaled to perform crypto load-balancing (host, lookaside, inline) and integrate with IKE clients.
- Core module:
  - Data-path(prepare/process) and SA management (create/destroy/update SA)
- Optional modules:
  - SA database with associated data path functions
  - SP database with associated data path functions
  - Crypto processing load-balancer
  - Shim layer for integration of library to existing external IKE solutions.



Low level pipeline with ipsec library



Security-Ipsec: how each fits together?

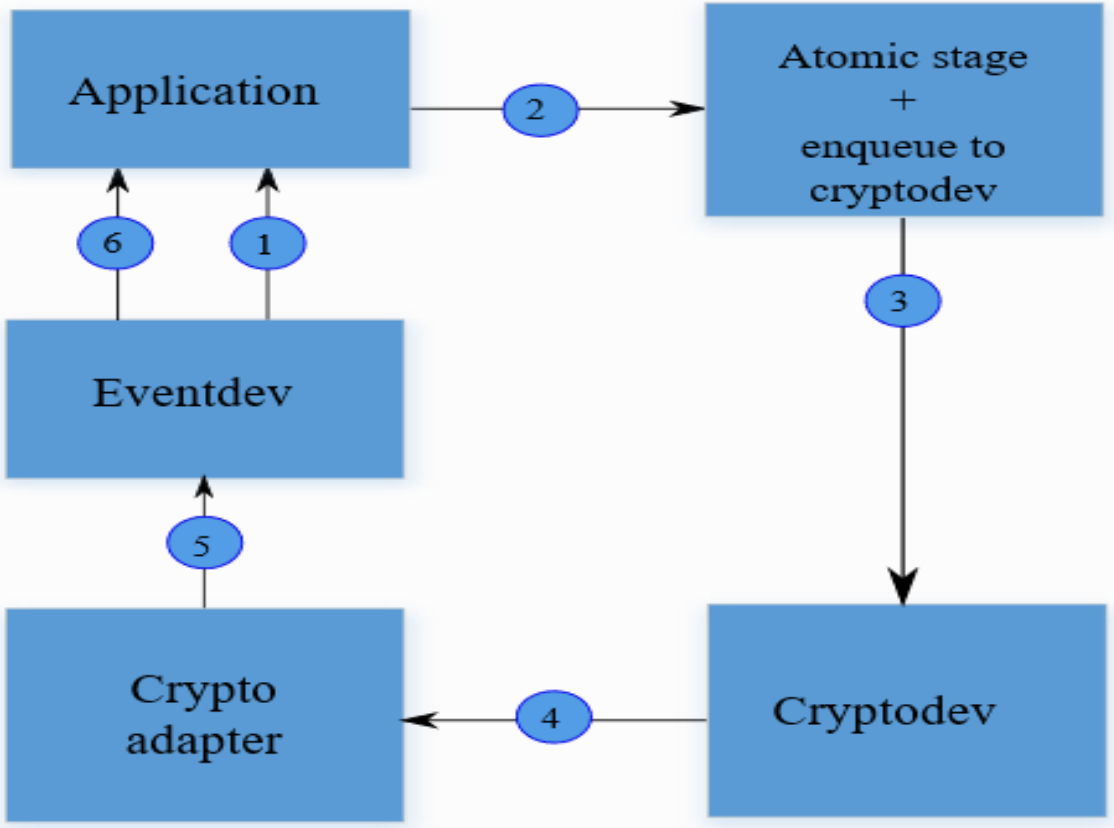
- Security provide control path APIs for session configuration which is used by the underneath driver to program Hardware.
- If the application chooses lookaside protocol offload or the inline protocol offload,
  - No requirement for ipsec Pre and Post processing.
- If Application chooses inline crypto or the basic crypto processing by the crypto device,
  - IPSec pre and post processing need to be done in the application.
  - rte_ipsec library provide generic data path APIs(prepare and process) for pre and post processing of protocol.
  - rte_ipsec library SA configuration APIs initializes the session information which is required for pre and post processing of crypto operation.


DPDK
DATA PLANE DEVELOPMENT KIT
EVENT CRYPTO
ADAPTER

Event Crypto Adapter

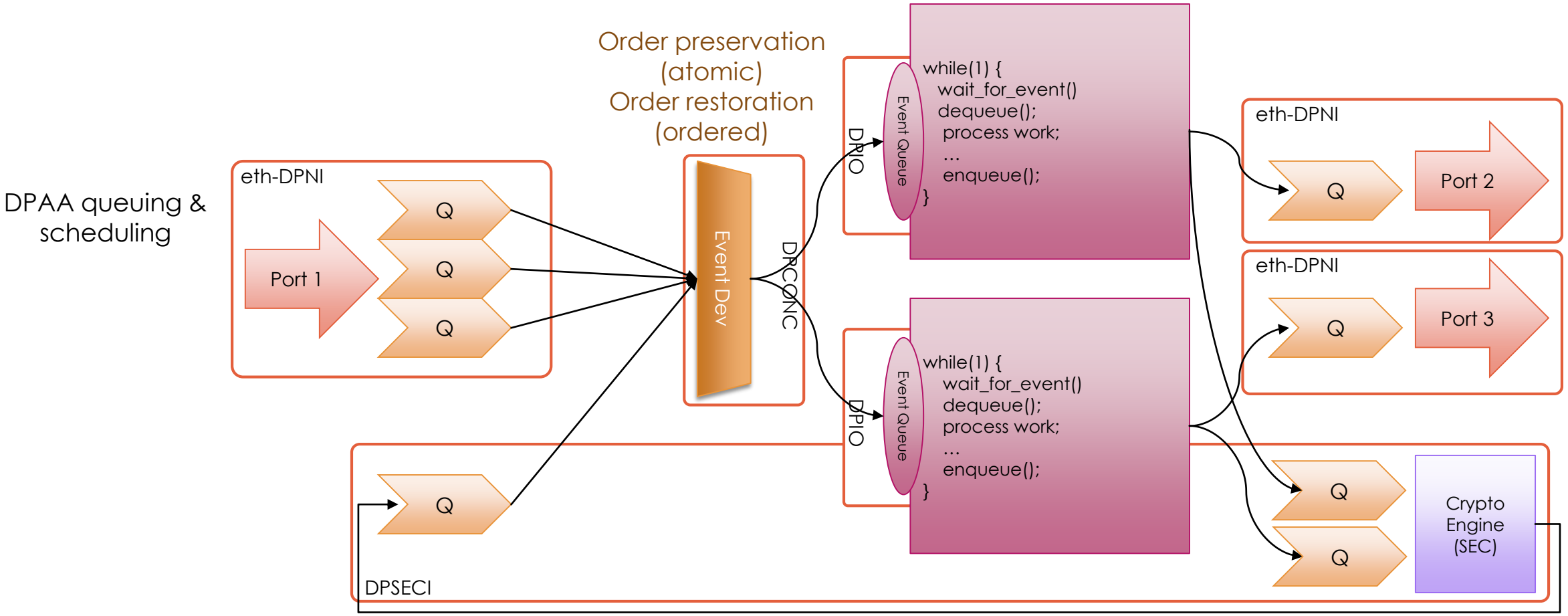
- Poll mode drivers means 100% CPU utilization irrespective of amount of traffic being processed.
  - DPDK now supports event based processing – no more wasted CPU cycles ☺
  - Each accelerator needs event adapter to connect eventdev
- Event crypto adapter adapts the crypto queues to work for event framework
- All crypto queues can be assigned to event device (hardware/ software scheduler)
- Event device schedule the traffic to multiple queues
- Support ordered, atomic and parallel queues
- Reduces CPU utilization when traffic is low
- Better utilization of hardware resources

Event Crypto Adapter processing



1. Application dequeues events from the previous stage
2. Application prepares the crypto operations.
3. Crypto operations are submitted to cryptodev by application..
4. Crypto adapter dequeues crypto completions from cryptodev.
5. Crypto adapter enqueues events to the eventdev.
6. Application dequeues from eventdev and prepare for further processing

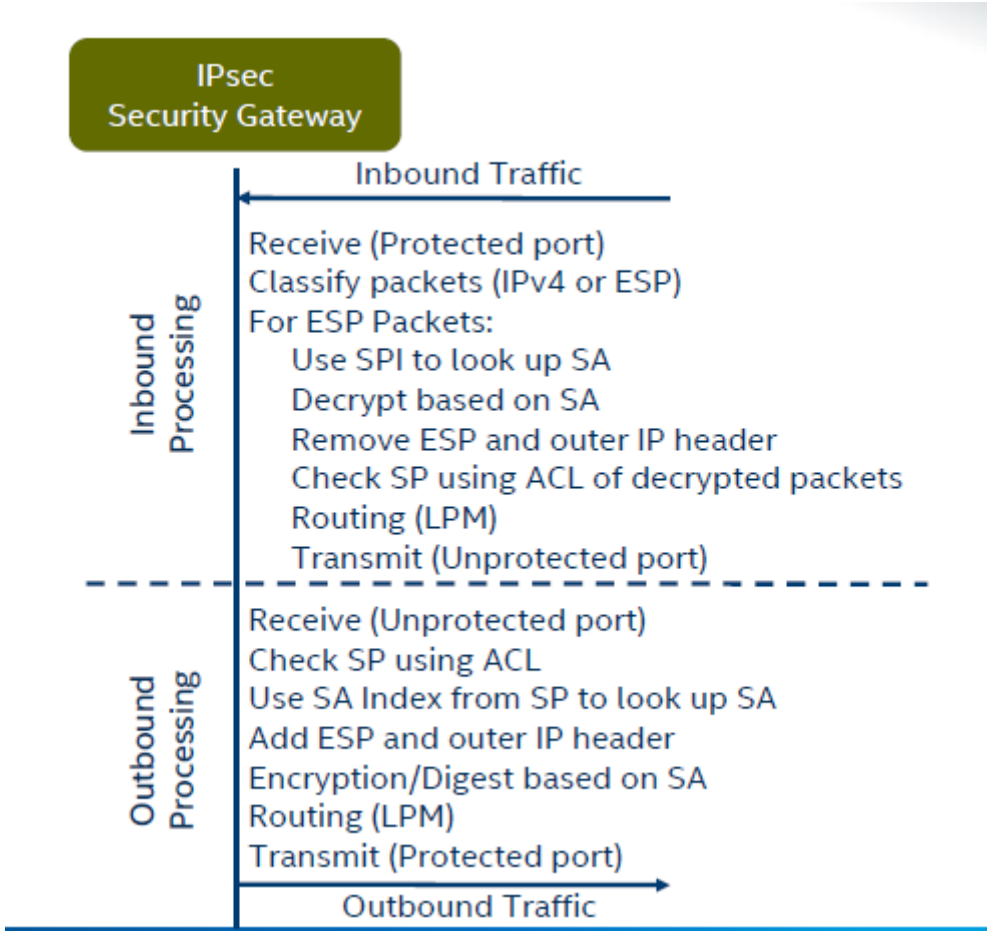
Crypto Adapter Example for NXP DPAA2 Platform



IPSEC Gateway Sample Application

IPSEC-SECGW *Sample* Application

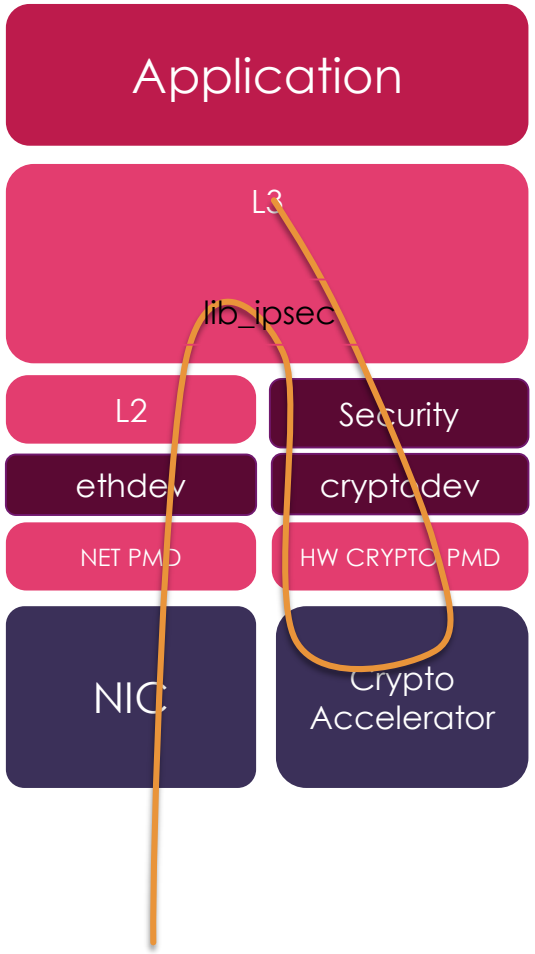
- Provide a L3 application for IPSEC forwarding
- Security Policies(SP) and Security Associations(SA) are manually configured using a cfg file.
- SPs are implemented as ACL rules
- SAs are stored in a table
- Routing is implemented using LPM
- Support all security acceleration modes.
- Support with and without IPSEC library
- Works well with both hardware and software devices



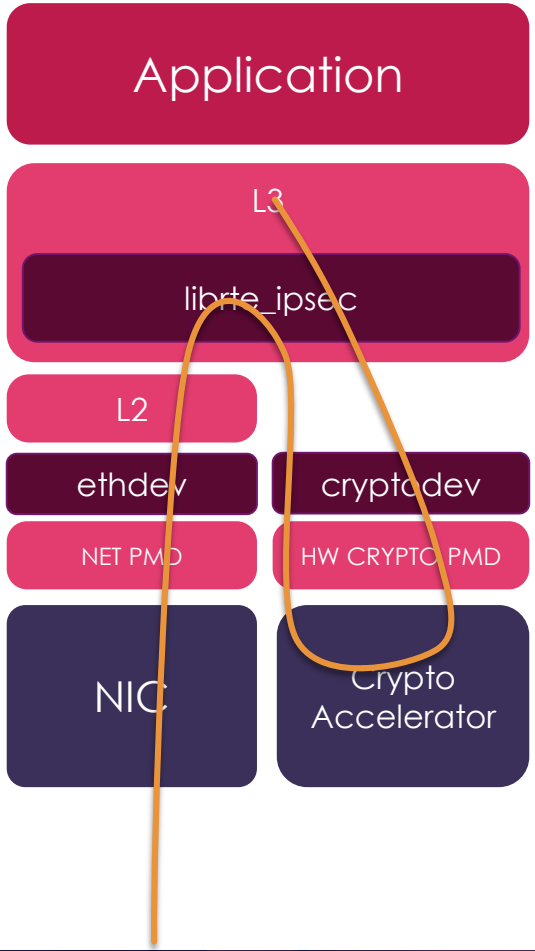
Supported_processing_modes

DPDK
DATA PLANE DEVELOPMENT KIT

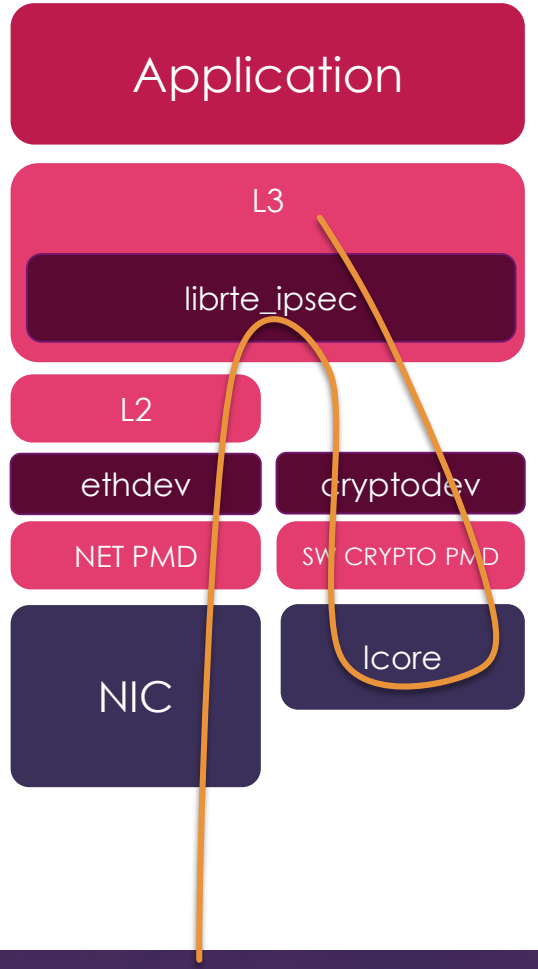
Lookaside Hardware Security Processing



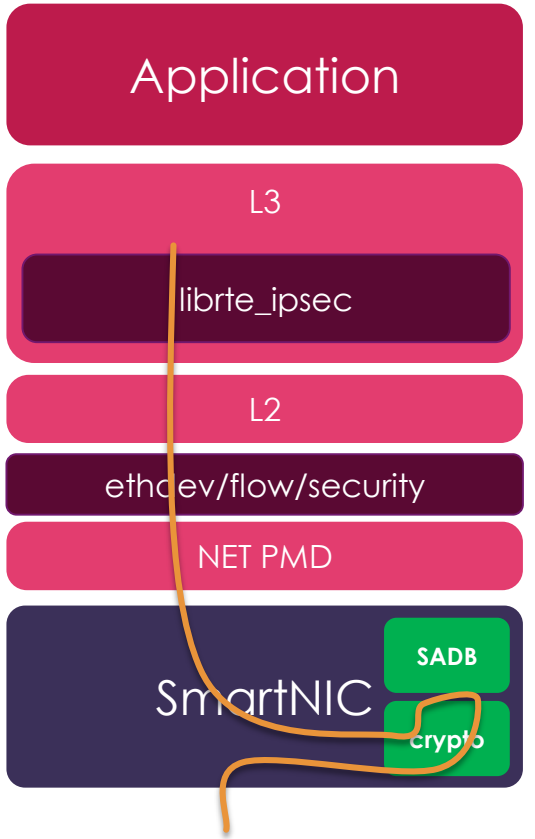
Lookaside Hardware Crypto Processing



Core based Crypto Processing



IO based Inline Crypto Processing



Future plan – 19.05 and above

- Event based IPsec application with ordered/atomic queue support
  - Data-path scaling, multicore processing of “Fat Flow” SA.
- Enhanced rte_ipsec library
  - AH transport/tunnel mode.
  - Full IPv6 support.
  - Fully migrate examples/ipsec-secgw to use librte_ipsec.
- High Level Data Path APIs.
- SAD APIs and database implementation.
- SPD APIs and database implementation.
- External IKE daemon integration.
- Enhanced armv8 crypto extension based library.

Questions?

Hemant Agrawal
<hemant.agrawal@nxp.com>

Akhil Goyal
<akhil.goyal@nxp.com>