

# SecY Interfaces

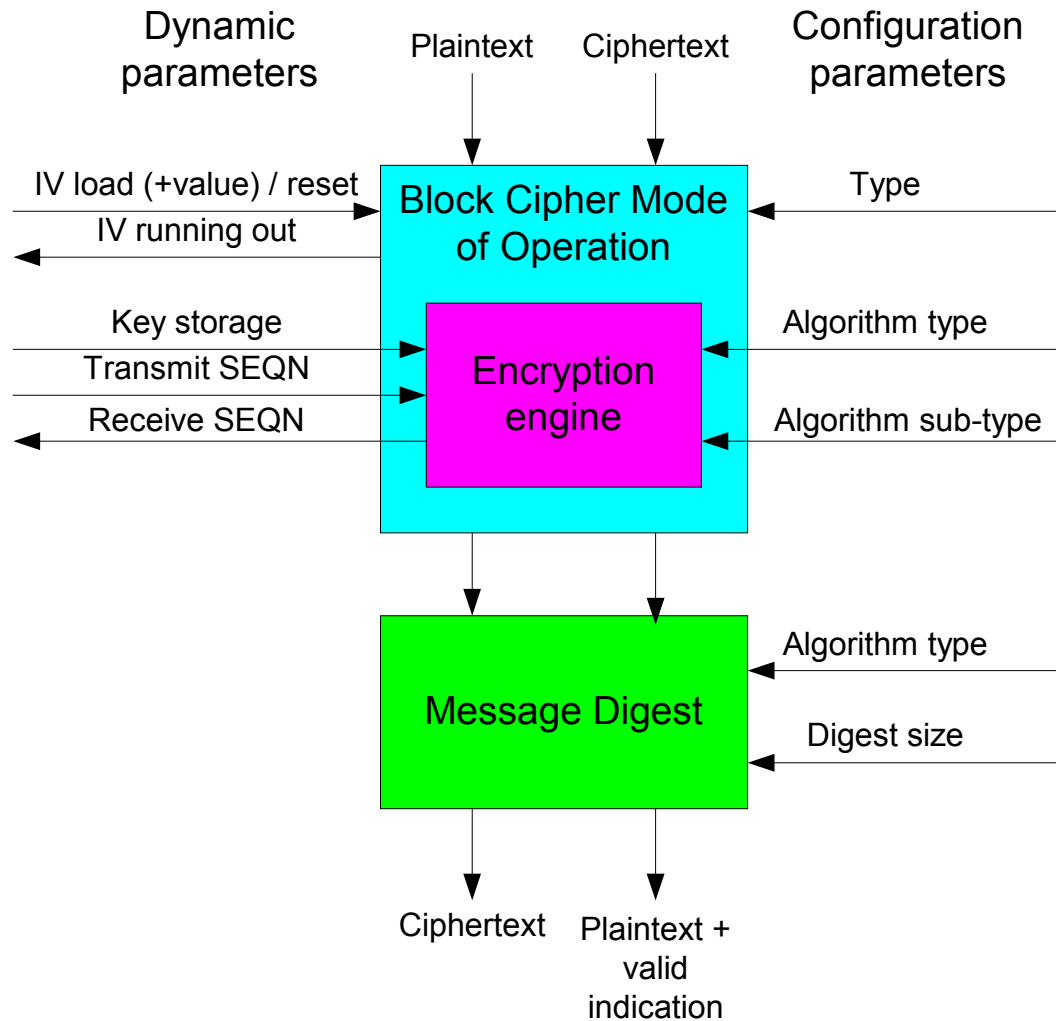
Onn Haran – Passave

# Interface Partition

---

- Two kinds of interfaces are required:
  - Static parameters agreed upon secure channel establishment (802.1aa??)
  - Dynamic parameters exchanged during secure channel operation (MACsec?)
- Key information is part of 802.1aa. Should it remain there or should it be part of MACsec?
- Interfaces are designed for maximal flexibility and future proof

# Assumed SecY Content



# Encryption Algorithm Requirement

---

- Encryption algorithm should be decided in negotiation stage
- Highest common denominator must be selected
- Algorithm type – identifies algorithm in use (for example: RC4, DES, AES)
- Algorithm sub-type – identifies version of algorithm in use (for example: AES-128, AES-192, AES-256)
- Block Cipher mode of operation – identifies mode in use (for example: CTR, OCB)
- Should flexibility be limited to avoid too many options?

# Message Authentication Requirement

---

- Message authentication algorithm should be decided in negotiation stage
- Highest common denominator should be selected
- Algorithm type – identifies algorithm in use (for example: MD5, SHA1)
- Digest size – identifies size reserved for digest (for example: 8 bytes, 10 bytes)
  - Typically it is a function of algorithm type, but for future proof it might be a parameter

# Key Exchange Requirement

---

- Key is exchanged dynamically during connection
- Two options exist for key storage:
  - Key is stored in SecY: Receiving a new key indication from MACsec/.1aa
  - Keys are stored in MACsec/.1aa: Receiving an array of keys
- Key storage must be limited → Width of key sequence number should be short (2 bits are sufficient)
- Sequence number for transmission should be given
- Output of SecY
  - Received Sequence Number
    - Used to detect key exchange

# Initialization Vector Requirement

---

- Some cipher block modes of operation require an initialization vector (IV)
- Some modes demand IV to be a secret, while other modes don't
- Preferably, a new IV will be delivered with every new key
- If IV does not need be a secret, then IV could just be reset with every new key
- Output of SecY
  - IV is running out: Need to initiate key exchange

# Static Parameters Summary

---

## Inputs

- Encryption Algorithm type
- Encryption Algorithm sub-type
- Block Cipher mode of operation type
- Message Authentication Algorithm type
- Message Authentication Digest size

# Dynamic Parameters Summary

---

## Inputs

- Key storage / Key message arrived
- Key Sequence Number to transmit
- Initialization Vector value / reset

## Outputs

- Received Key Sequence Number
- IV is running out