

# SecY Interfaces

Version 4

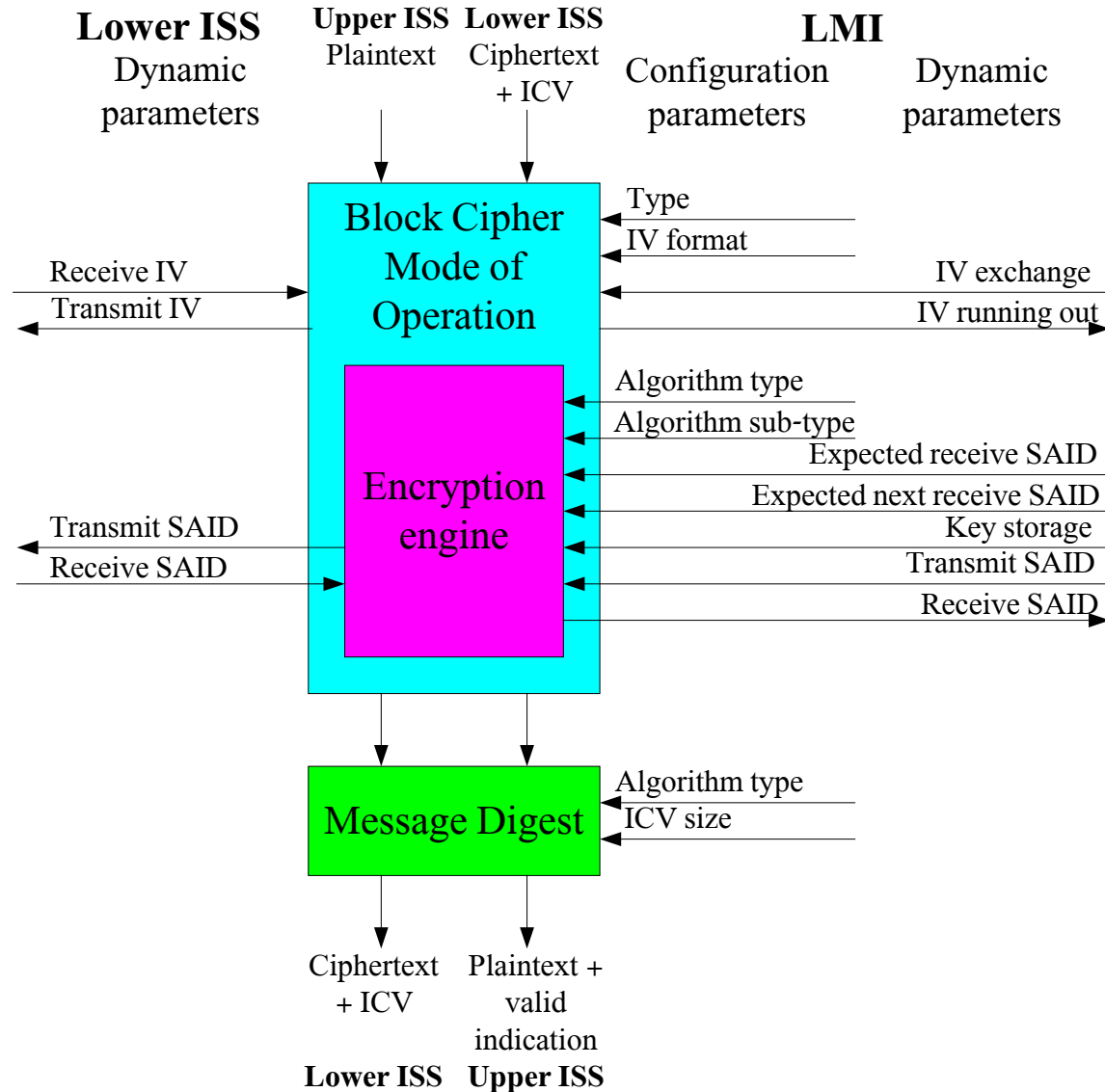
Onn Haran – Passave

# Interface Partition

---

- Two kinds of interfaces are examined:
  - LMI – Layer Management Interface (802.1aa)
    - Static parameters agreed upon secure channel establishment
    - Dynamic parameters exchanged during secure channel operation not tightly synchronized with data delivery
  - Lower ISS (MACsec)
    - Dynamic parameters exchanged during secure channel operation tightly synchronized with data delivery
- 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: NULL, RC4, DES, AES)
  - AES is the default algorithm
- 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?

# Integrity Check Value Requirement

---

- Integrity check value algorithm should be decided in negotiation stage
- Highest common denominator should be selected
- Algorithm type – identifies algorithm in use (for example: MD5, SHA1, checksum of block cipher mode of operation)
- ICV size – identifies size reserved for ICV (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
- Keys are stored in .1aa
  - Receiving an array of keys
  - At least current and new key
  - Preferably not more than current and new key
- SAID for transmission should be given
- Expected values of current and next SAID are given to filter non-matching frames
- Output of SecY
  - Received SAID: used to detect key exchange

# Initialization Vector Requirement

---

- Some cipher block modes of operation require an initialization vector (IV)
- IV (entirely or partly) is transmitted as part of SMPDU
- When only part of IV is transmitted, behavior of remaining bits is agreed upon channel establishment (for example: zero padded, fixed value, increased upon wrap-around)
- IV width is agreed upon channel establishment
- Transmitted IV could be exchanged (reset / reloaded) dynamically, preferably synchronized with key exchange
- Output of SecY
  - IV is running out: Need to initiate key exchange
    - Output might not be necessary if requirements from key exchange scheduler are stated correctly

# Relationship to Ciphersuite

---

- This presentation doesn't contradict ciphersuite concept
- Without ciphersuite each parameter is negotiated independently
- With ciphersuite all parameters are negotiated together
- I believe that all parameters should be specified for clarity even if ciphersuite concept is used



# LMI Static Parameters Summary

---

## Inputs

- Encryption Algorithm type
- Encryption Algorithm sub-type
  
- Block Cipher mode of operation type
- IV width
- IV remaining bits behavior
  
- ICV Algorithm type
- ICV size

# LMI Dynamic Parameters Summary

---

## Inputs

- Key storage
- SAID to transmit
- Expected receive SAID
- Expected next receive SAID
  
- Initialization Vector exchange

## Outputs

- Receive SAID
- IV is running out

# Lower ISS Parameters Summary

---

## Inputs

- Ciphertext + ICV
- Receive IV
- Receive SAID

## Outputs

- Ciphertext + ICV
- Transmit IV
- Transmit SAID