

SecY Interfaces

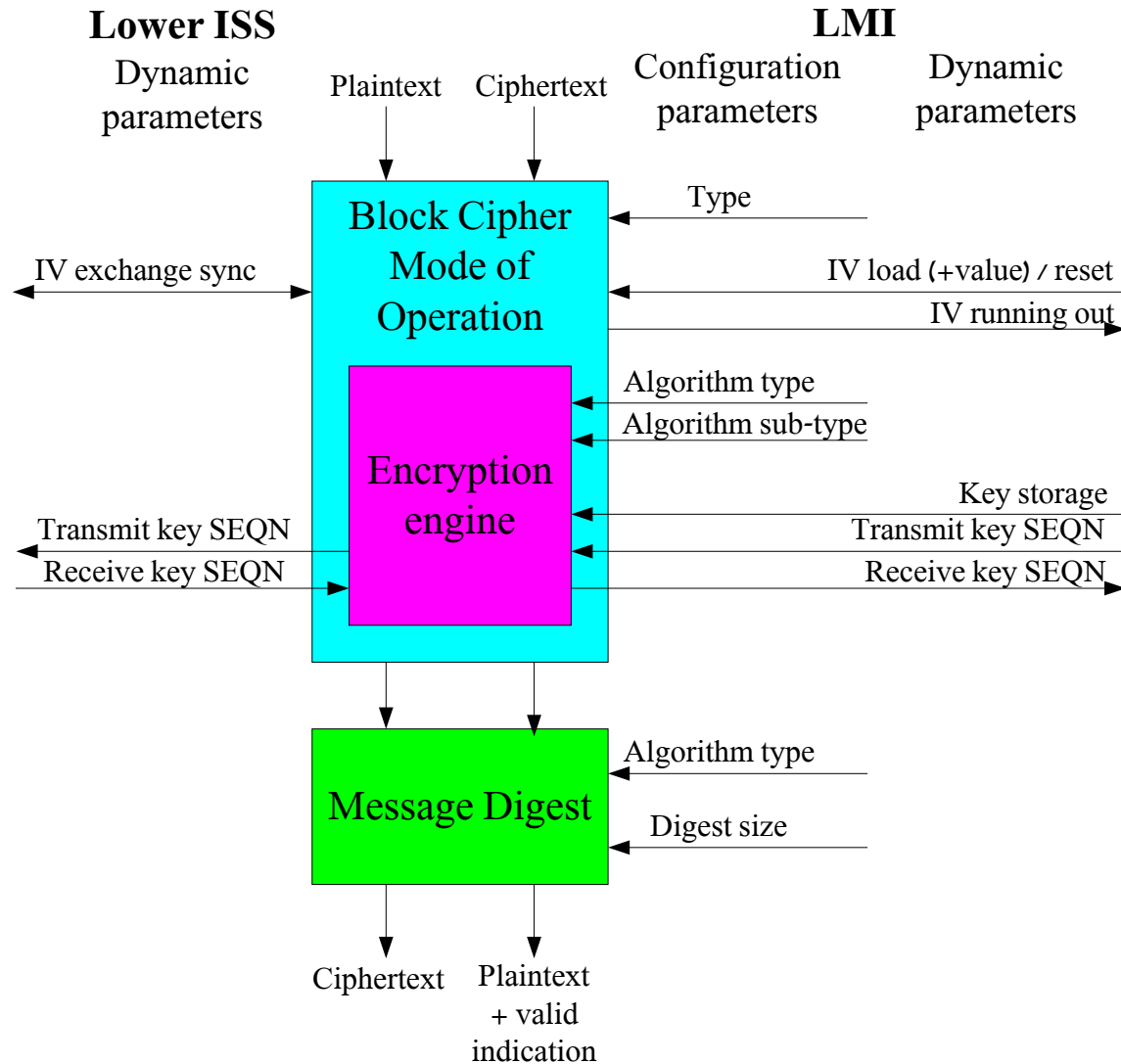
Version 2

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)
- 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
- Keys are stored in .1aa: Receiving an array of keys
 - At least current and new key
- Key storage must be limited → Width of key sequence number should be short
- Key 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
- IV exchange should be tightly synchronized with data delivery
- 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

LMI 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

LMI Dynamic Parameters Summary

Inputs

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

Outputs

- Received Key Sequence Number
- IV is running out
 - Might be replaced with requirements from key exchange scheduler

Lower ISS Parameters Summary

Inputs

- IV exchange sync
- Received Key Sequence Number

Outputs

- IV exchange sync
- Key Sequence Number to transmit