MACsec and MAC Data Security Nonce construction

Active meeting discussion facilitated by these slides, do not expect any consistency or completeness ..

Mick Seaman
mickseaman@gmail.com

GCM-AES-128 Nonce

The existing MACSec nonce:

96-bit Nonce = PN (32 bits) || SCI (64bits)

SCI either in the SecTAG (has to be if not from end station – take from SA + Port ID 1, and not p2p – take from Key Agreement).

GCM-AES-XPN Nonce

The existing MACSec nonce:

96-bit Nonce = (XPN (64 bits) || SSCI (32 bits)) + Salt (96 bit)

SSCI assigned by Key Agreement protocol (convention or explicit) from 64-bit SCI

SCI either in the SecTAG (has to be if not from end station – take from SA + Port ID 1, and not p2p – take from Key Agreement).

Ascon Nonce (proposed)

MACSec nonce:

128-bit Nonce = (XPN (48 bits) || SCI (64 bits) || KN (16 bit) + Salt (128 bit)

SCI either in the SecTAG (has to be if not from end station – take from SA + Port ID 1, and not p2p – take from Key Agreement).

MAC Data Security Nonce (proposed)

As per related MACsec Cipher Suites

If a station has two independent crypto engines using the same SAK must use a different nonce space for each.

SCI (64 bits) in the SecTAG.

(has to be if not from end station – take from SA + Port ID 1, and not p2p – take from Key Agreement).