Frame Format for IEEE 802.1AEdk MACsec Privacy

Don Fedyk LabN Consulting L.L.C

dfedyk@labn.net

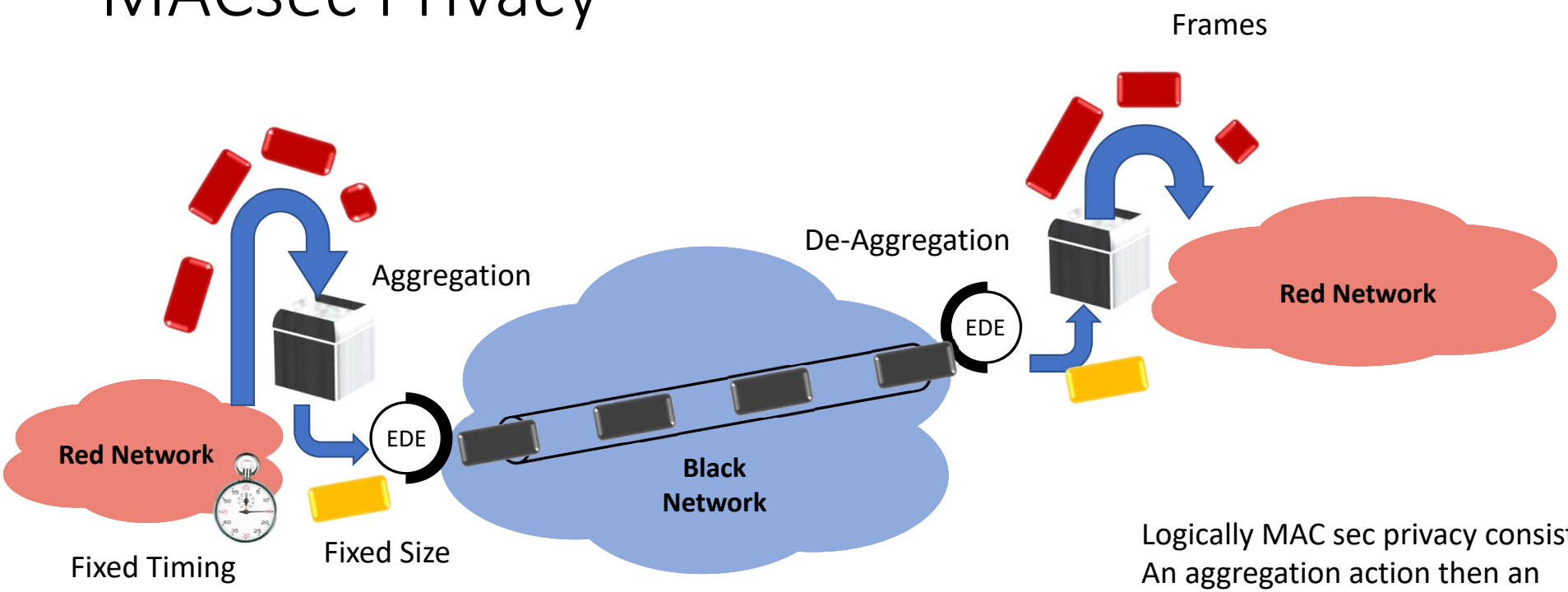
Outline

- Problem Statement
- Some possible formats
- Requirements review
- Alternatives
- Discussion

Problem Statement

- MACsec Privacy option by anonymizing MACsec frames with fixed size and fixed timing
- Reduce inefficiency by packing smaller frames and optionally fragmenting frames
- Make use of existing MACsec EDEs
- Material Already presented
  - http://www.ieee802.org/1/files/public/docs2019/new-fedyk-traffic-flow-security-0219.pdf
  - http://www.ieee802.org/1/files/public/docs2019/dk-seaman-mac-privacy-0909-v01.pdf

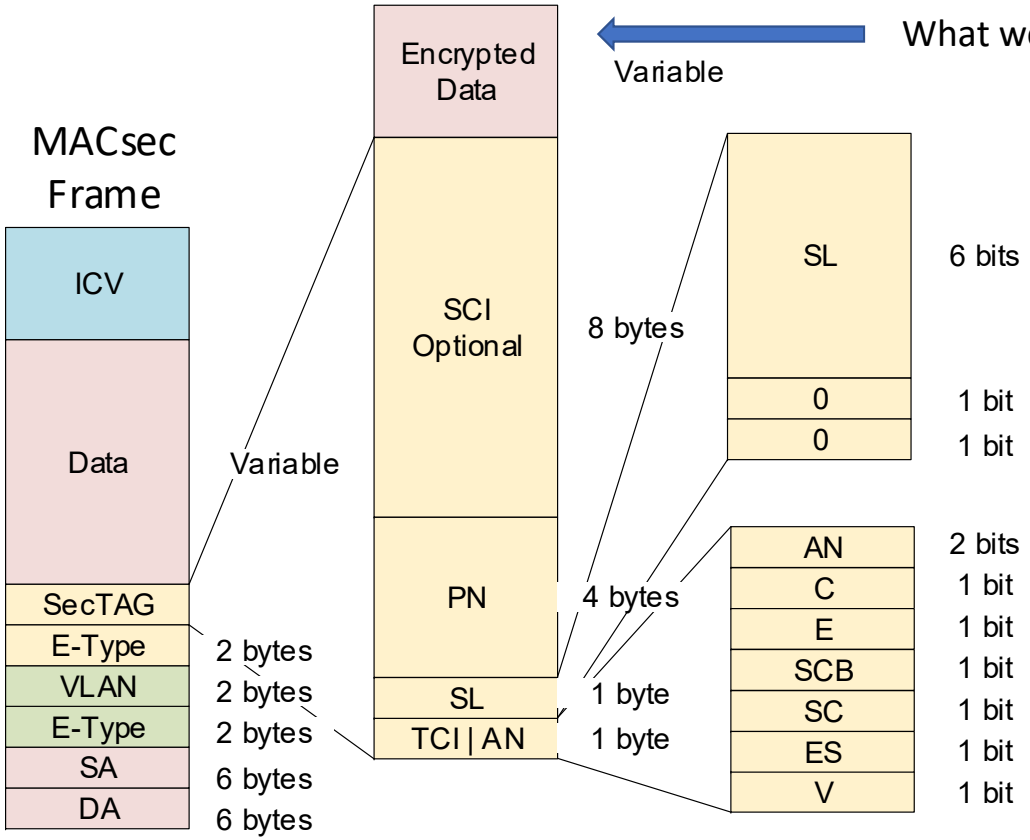
MACsec Privacy



MAC Privacy Packet Data Units

Logically MAC sec privacy consist of An aggregation action then an Encryption action even though they may be highly integrated the separation allows the use of exiting MACsec capable devices.

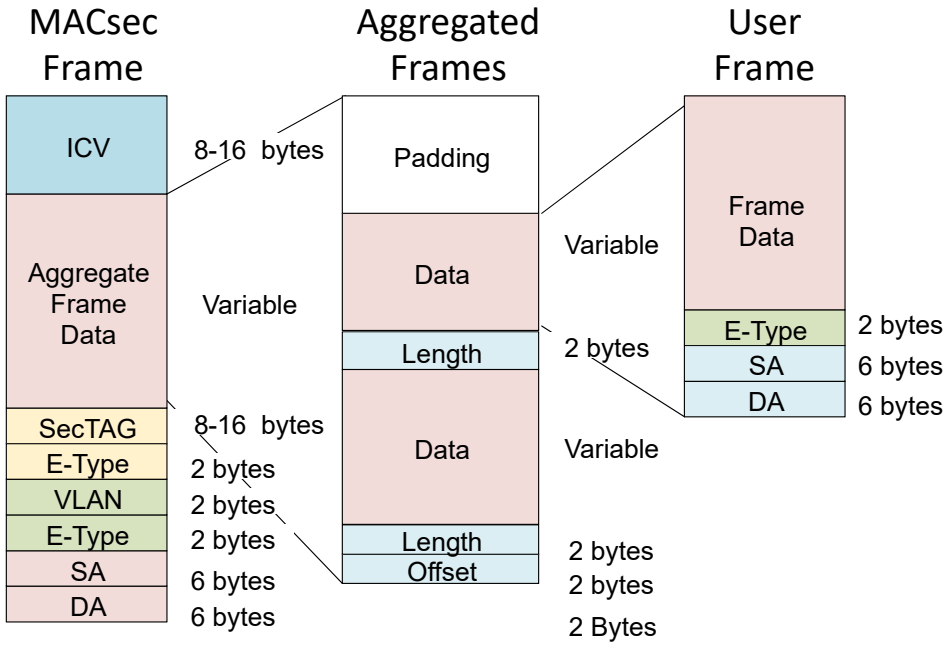
MACsec Frames – MAC Privacy



DA	Destination Address
SA	Source Address
E-Type	Ethernet Type
VLAN	Virtual Local Area Network
SecTAG	Security TAG

Existing SecTAG (Yellow) stays the same

Nonstandard Ethernet Security Specification (ESS) Format



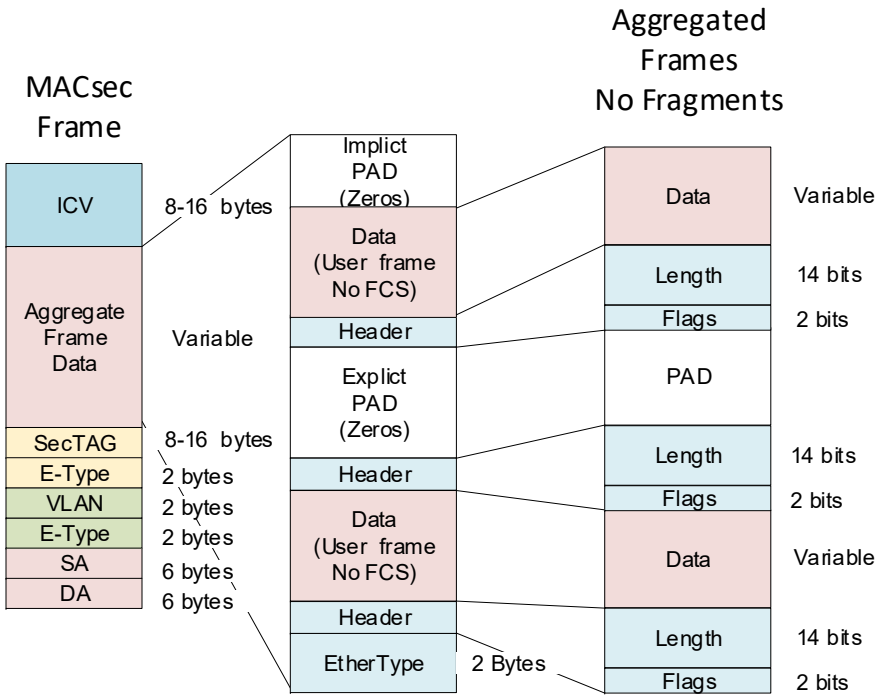
DA	Destination Address
SA	Source Address
E-Type	Ethernet Type
VLAN	Virtual Local Area Network
SecTAG	Security TAG

Notes

This format is the original ESS format
It has one main issue and two minor ones:

1. If the aggregation is performed separately from the encryption – there is no packet number (sequence number)
2. The padding is not optimized for recognition when there is no data following padding (makes late addition hard)
3. There is no traffic class mapping, so all aggregated frames are one priority.
4. Ethertype if using an existing MACsec implementation

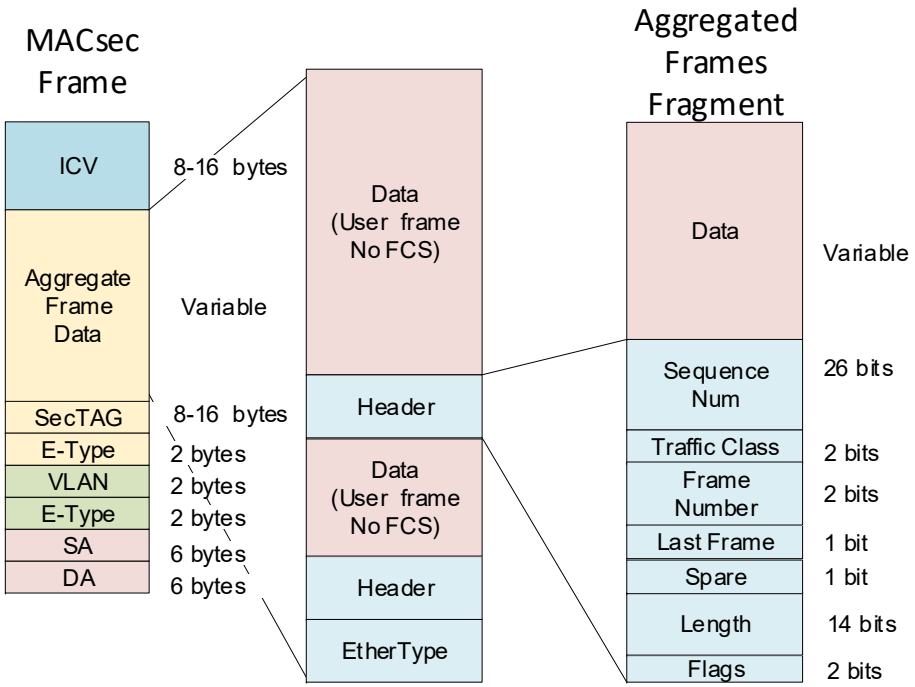
Mick's Proposal (Sept Interim)



DA	Destination Address
SA	Source Address
E-Type	Ethernet Type
VLAN	Virtual Local Area Network
SecTAG	Security TAG

- Small Frames single payload
- 16 bytes overhead header
- Implicit Padding at end of MPPDU frame
- Explicit Padding option in Frame – allows data to be added as frame is being transmitted if there is room.

Mick's Proposal (Sept Interim)

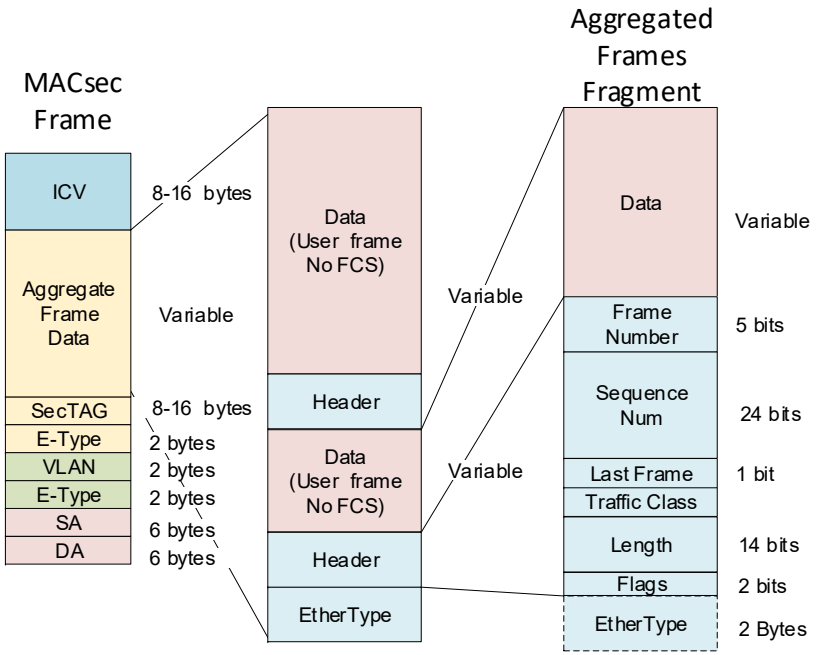


DA Destination Address
SA Source Address
E-Type Ethernet Type
VLAN Virtual Local Area Network
SecTAG Security TAG

Fragments

- Allow longer frames
- Up to 4 fragments
- Sequence number / traffic class
- Allow traffic classes (4)
- Shares common header with unfragmented frames

Modified Proposal for Fragments



DA	Destination Address
SA	Source Address
E-Type	Ethernet Type
VLAN	Virtual Local Area Network
SecTAG	Security TAG

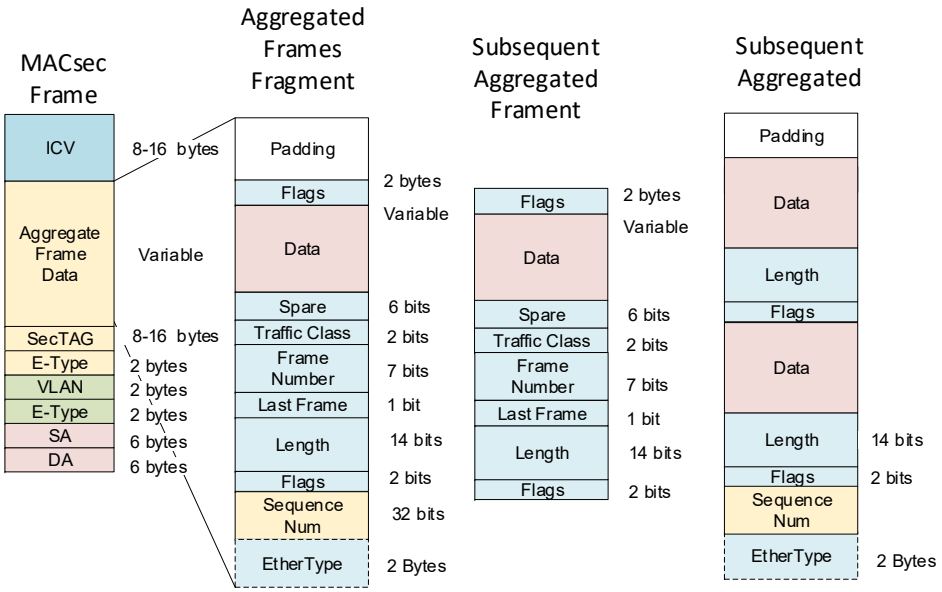
Fragments

- Allow longer frames
- Up to 32 fragments
- Sequence number / traffic class
- Sequence number plus frame number is 1 - 29 bit number per fragmented frame
- Last frame bit + 29 bits identifies last frame.
- Allow traffic classes (4)
- Shares common header with unfragmented frames

Requirements

- Support wide range of MACsec frame sizes 256 – 9K bytes
- Support Fragmentation of user frames into MACsec
- Support separate aggregation and encryption
  - Means the PN (sequence number) of MACsec is not available for Fragmentation
  - Sequence number (of sorts) required for fragmented Frames
- Support Late addition of Frames in MPPDU
  - Frames may be included in a MACsec frame that has begun transmission but has available space in the bits not transmitted.
  - May be performed wherever the MPPDU is encoded.
  - Also requires more shorter fragments if preemptions is allowed
- New MACsec Ethernet type for MACsec carrying MPPDUs

An alternative



This proposal is functionally equivalent but allows

- 2 byte overhead for fragments
- 2 byte header for all aggregated frames
- One Sequence number per frame
- 32 bits – 4 Billion frames
- Caveat Sequence logic becomes more complex
- Lost frames results in all fragments in process being dumped regardless of Traffic class. Frame sequence + fragment number is not as absolute as per TC Fragment sequence + fragment number.
- Lost frames are always detected up to the sequence rollover.

Discussion

- How Big should sequence number be?
- Largest Frame Non-Fragmented
  - Jumbo – MACsec header – 6 bytes
- Largest Fragmented Frame
  - 32 x MPPDU Frame size
- Lost Fragments
- Lost Frames
- Mis-ordered Frames
- Other?

Glossary New Terms for MAC sec Privacy

MPDU - MACsec Protocol Data Units

TCI – TAG Control Information

SL – Short Length

PN - Packet Number

SCI – Secure Chanel Identifier Optional

MPPDU – MAC Privacy PDU – strawman term

MPPCI – MAC Privacy PDU Component Identifier –strawman term

(MTDU – MACsec Tunnel data Units – Industry term = MPPDU)

(MSDU – MACsec Secure Data Unit – Industry term = MPPCI)