DTLS 1.3

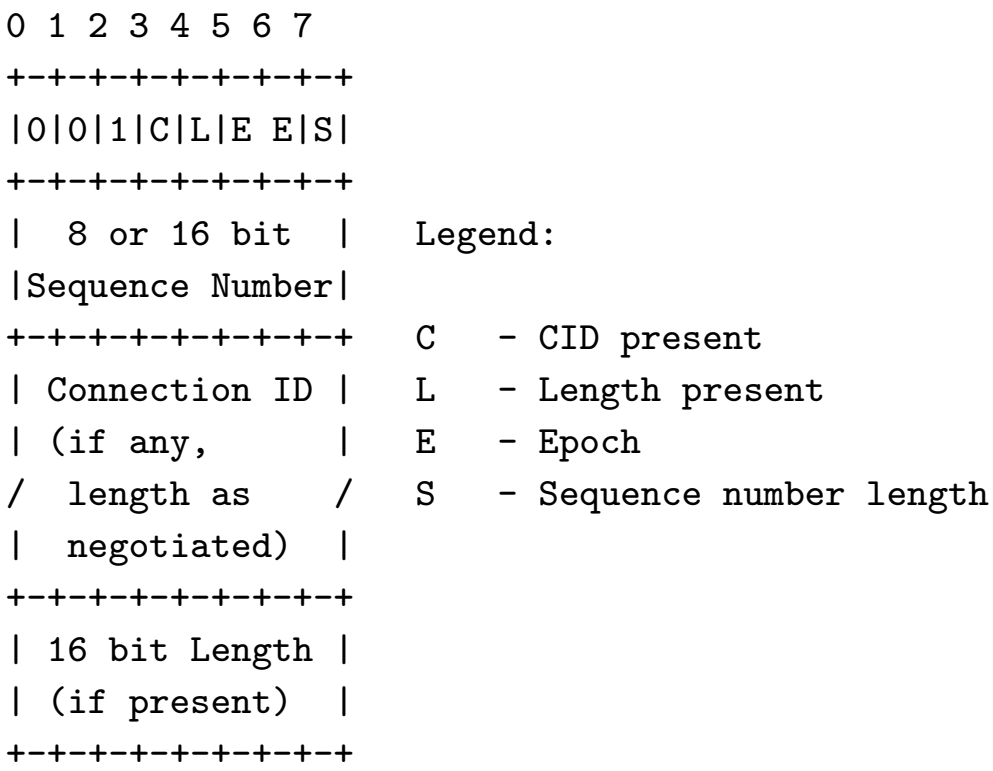
draft-ietf-tls-dtls13-28

Eric Rescorla
Mozilla
ekr@rtfm.com

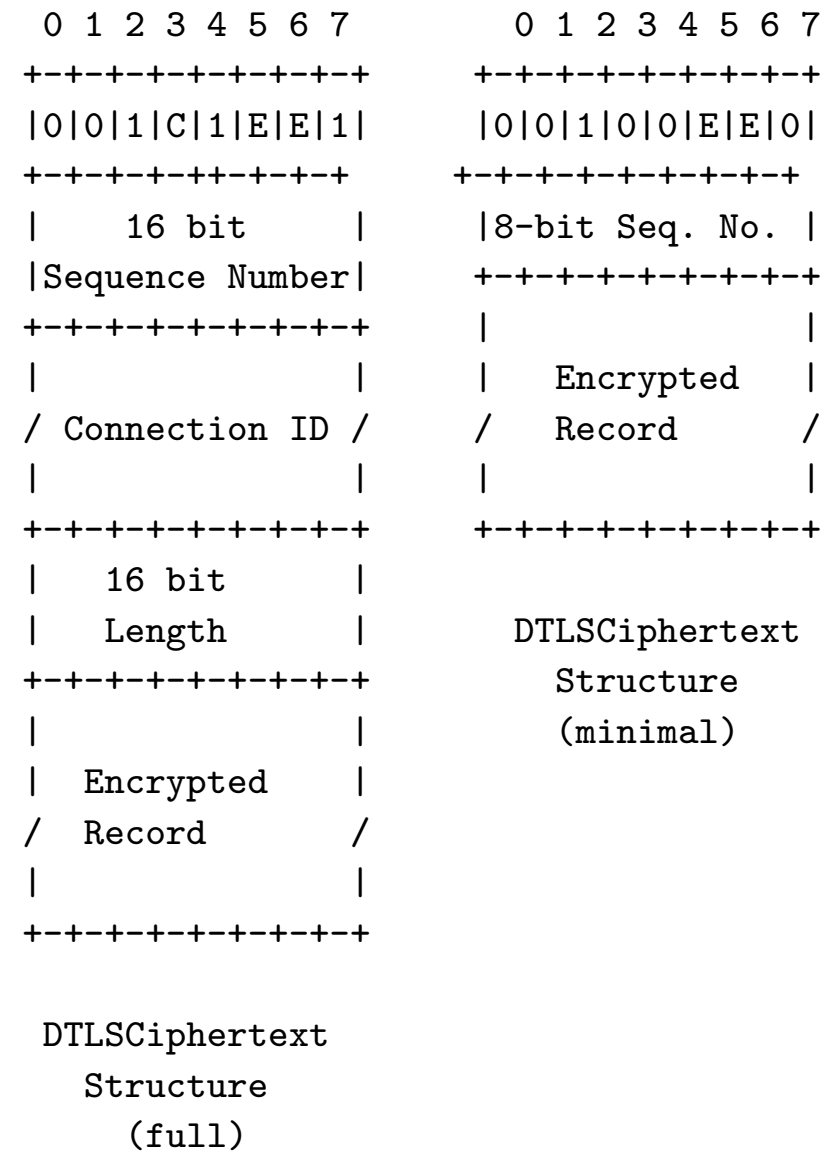
Hannes Tschofenig
Arm Limited
hannes.tschofenig@arm.com

Nagendra Modadugu
Google
nagendra@cs.stanford.edu

DTLS 1.3: Unified Packet Format (New)



Examples


0 1 2 3 4 5 6 7
0 0 1 C 1 E E 1
16 bit
Sequence Number
Connection ID
16 bit
Length
Encrypted
Record
DTLSCiphertext
Structure
(full)
0 1 2 3 4 5 6 7
0 0 1 0 0 E E 0
8-bit Seq. No.
Encrypted
Record
DTLSCiphertext
Structure
(minimal)

Record Sequence Number Encryption

- Borrowed from QUIC
- Client and server derive a `sn` key
  - Generate *mask* by enciphering the first bytes of the ciphertext with `sn` key
  - XOR the mask with the SN
- Important change: MUST validate record MAC before rejecting duplicates

Compatibility Mode

- DTLS 1.3 MUST NOT use compatibility mode.
- That is all.

End of EOED (PR#62

- It's not clear we need EOED in DTLS
  - Epoch tells you when to switch to handshake data
  - DTLS is lossy anyway so truncation attacks don't apply
- Loss of EOED causes blocking
  - So this is irritating
  - QUIC removed it
- Proposal: Remove EOED from DTLS 1.3
  - Note: this affects the transcript

Connection ID Flexibility (PR#65)

- Previously all the CID management messages were one at a time
  - Issuing N CIDs means sending N `NewConnectionId` messages
  - What about reordering?
- Proposal
  - `NewConnectionId` can have an arbitrary number of CIDs
  - `RequestConnectionId` has a count
  - Only one of each outstanding at once

Other Issues?