# Connection ID

`draft-ietf-tls-connection-id-01`

**Eric Rescorla**
Mozilla
ekr@rtfm.com

Hannes Tschofenig
Arm Limited
hannes.tschofenig@arm.com

Thomas Fossati
Nokia
thomas.fossati@nokia.com

Tobias Gondrom
Huawei
tobias.gondrom@gondrom.org

# Reminder: IETF 101

- Explicitly mark the presence of CID
  - CID length is implicit
- Split work into DTLS 1.2 and DTLS 1.3
  - Conn-ID document becomes DTLS 1.2 only
  - Add conn ID to DTLS 1.3 main draft
  - Both use the "connection_id" extension

# DTLS 1.2: CID "present" marking

- Two options presented
  - Bit in the length field
  - Shadow content type values
- Concern about compat of length field $\rightarrow$ shadow content types
- Spec defines four new types (alert, handshake, application, heartbeat)
  - This does seem like a lot

# Alternate Design (Thomson)

- Allocate one extra code point ("encrypted content type + CID")
  - This would use TLS 1.3-style content type encryption
  - + Free padding
  - So no need for more code points

# Alternate Alternate Design

```
struct {
      ContentType type = XX; // new type value
      ProtocolVersion version;
      uint16 epoch;
      uint48 sequence_number;
      ContentType true_content_type;
      opaque cid[cid_length];                  // New field
      uint16 length;
      select (CipherSpec.cipher_type) {
          case block:  GenericBlockCipher;
          case aead:   GenericAEADCipher;
      } fragment;
} DTLSCiphertext;
```

# Other ideas?

# DTLS 1.3

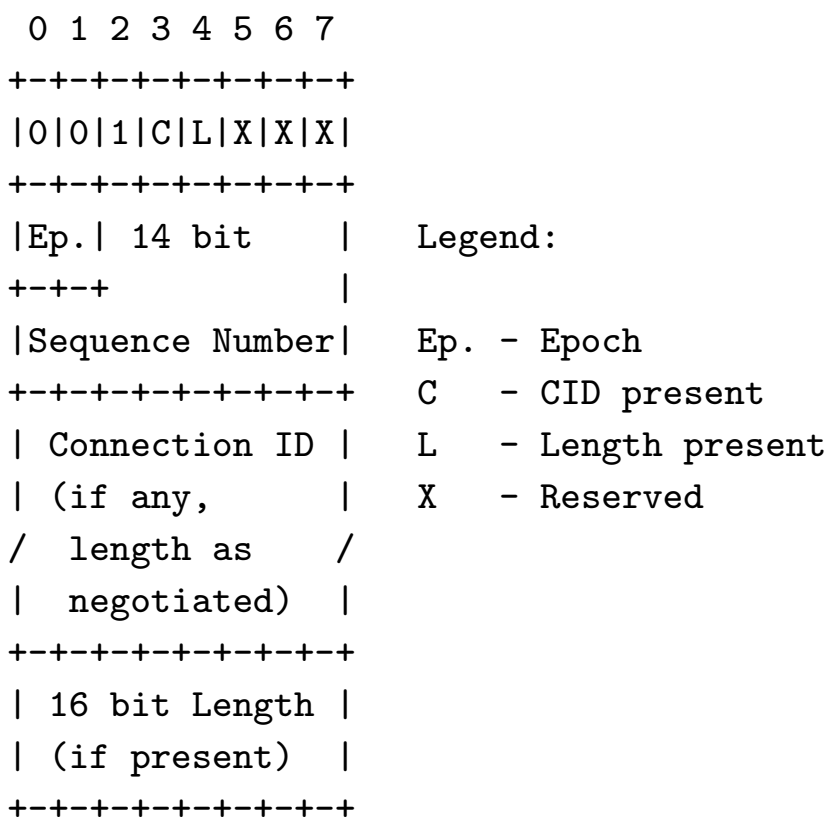
draft-ietf-tls-dtls13-28

**Eric Rescorla**
Mozilla
ekr@rtfm.com

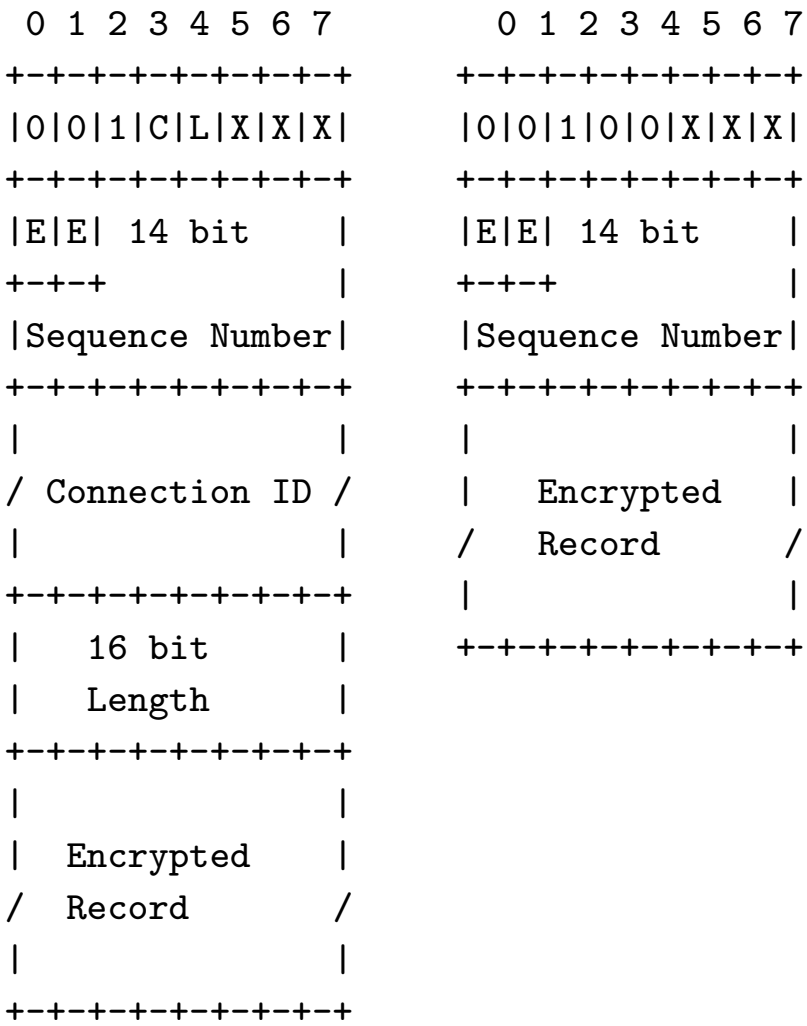
Hannes Tschofenig
Arm Limited
hannes.tschofenig@arm.com

Nagendra Modadugu
Google
nagendra@cs.stanford.edu

# DTLS 1.3: Unified Packet Format



# Examples


0 1 2 3 4 5 6 7
0|0|1|C|L|X|X|X|
E|E| 14 bit
Sequence Number
Connection ID
16 bit
Length
Encrypted
Record
0 1 2 3 4 5 6 7
0|0|1|0|0|X|X|X|
E|E| 14 bit
Sequence Number
Encrypted
Record

# New Connection IDs

- DTLS 1.3 still has a new connection ID message
- Also a `RequestConnectionId` message (new)
  - Semantics: please send a new spare CID

# What about Record Sequence Numbers?

- New CIDs are good but sequence numbers leak relationships
- Solution: QUIC-style packet number encryption for all DTLS 1.3 ciphertext packets (with our without CID)
  - Use some of the ciphertext as the input to a PRF (?)
  - XOR PRF output with the RSN
  - (can be emulated with counter mode)
- Drafty draft PR at
  `https://github.com/tlswg/dtls13-spec/pull/48`

# Other Issues?