DTLS CID open issue

---

Eric Rescorla
ekr@rtfm.com
MAC Construction (MtE)

\[ \text{MAC(MAC\_write\_key, ...} \]

\[ \text{cid + cid\_length +} \]

\[ \text{length of (IV + DTLSCiphertext.\text{enc\_content}) + ...}) \]

- **CID length is known externally**
  - and is encoded after the CID
- **This is not injective**
- **01 01 02 00 03 ... could be:**
  - CID = 01, length = 2000, payload = 03...
  - CID = 0102, length = 0003
Not Clear What the Impact Is

- The Finished covers the CID exchange
  - but the CID is used in the record containing the Finished
- But generally just seems unattractive
- So we should probably fix it
- Shouldn’t be an issue for TLS 1.3 (or AEAD)
Proposed MAC Input (AtE)

```c
struct {
    uint8 marker = tls12_cid;
    uint8 cid_len;
    uint8 content_type = tls12_cid;  \
    uint16 DTLSCiphertext.version;  |  appears on wire
    uint64 seq_num;  // includes epoch  |
    opaque cid[cid_len];  |
    uint16 length_of_DTLSInnerPlaintext;
    DTLSInnerPlaintext.content;  \ 
    DTLSInnerPlaintext.real_type;  |  entirety of DTLSInnerPlaintext
    DTLSInnerPlaintext.zeros;  |
};
```

Similar approaches for AEAD and MtE
Objections?