Compact TLS draft-08

Eric Rescorla, Richard Barnes, Hannes Tschofenig, Ben Schwartz

TLS WG @ IETF 116, March 2023

Rev 2

Minor changes since IETF 114 (draft-06)

- **New field**: `CTLSExtensionTemplate.self_delimiting_extensions`
  - From review for formal analysis by Théophile Wallez (INRIA).
  - Ensures both sides agree on which extensions don’t need a length prefix.
- Pinning the `pre_shared_key` extension in the cTLS Template is **prohibited**.
  - Credit to Ilari Liusvaara for pointing out that this extension needs special handling.
- Lots of minor editorial changes and cleanups
  - No more discussion of elliptic curve compressed representations. This can be handled independently of cTLS.
  - Reworked examples.
  - More guidance and explanation on various points.

Status

- Formal analysis ongoing and early results look promising (with one change already in cTLS-08).
- Implementation work ongoing (by Hannes).
  - Please ping us to do interop testing.

Open Issues

- #80: Is there any possibility of confusion about:
  - whether a supported `NamedGroup` produces fixed-length `key_exchange`s?
  - whether a supported `SignatureScheme` produces fixed-length `signature`s?
- #87: How should the registry of well-known cTLS profiles work?
  - Can we reasonably embed the entire profile JSON blob into each row in the registry?
  - Can we impose some restrictions on registered profiles (e.g., no certificates)?
    - How does this interact with a FCFS policy?
- #77: Racing mirror-image handshakes on an undirected 5-tuple
  - (Accidentally) works in DTLS, but doesn't work in Datagram cTLS.
  - Should we spend a `ContentType` codepoint or 2 bytes of handshake to make this work?
- #71: Decide what to with `epoch` on streaming transports where it isn't needed.

close_notify