

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`

-31 Draft

- A lot of editorial improvements (thanks MT, others)
- Update the example

Issue 78 – amplification factor

- QUIC goes to a lot of effort to avoid amplification from small ClientHellos
- DTLS historically vague on this (HRR not required)
- Definitely not an issue in some scenarios (w/ ICE)
- Should we do something here?
- Proposal: SHOULD-level requirement to do HRR in “sensitive” cases.

Issue 76 – non-empty cookies + cookie extension

- There's no good reason for this
- Proposal: Forbid this and require rejection

Issue 72: Key Separation

- Do we need key separation with TLS?
- The transcript is different (headers)
- Proposal: Do nothing

Implementation Status

- Implementations in NSS, Mint, mBed
- Initial interop between Mint and NSS (mBed coming soon)

Next Steps

- Update the issues as discussed above
- New draft
- Get more interop – implementation report on the list
- Send to IESG