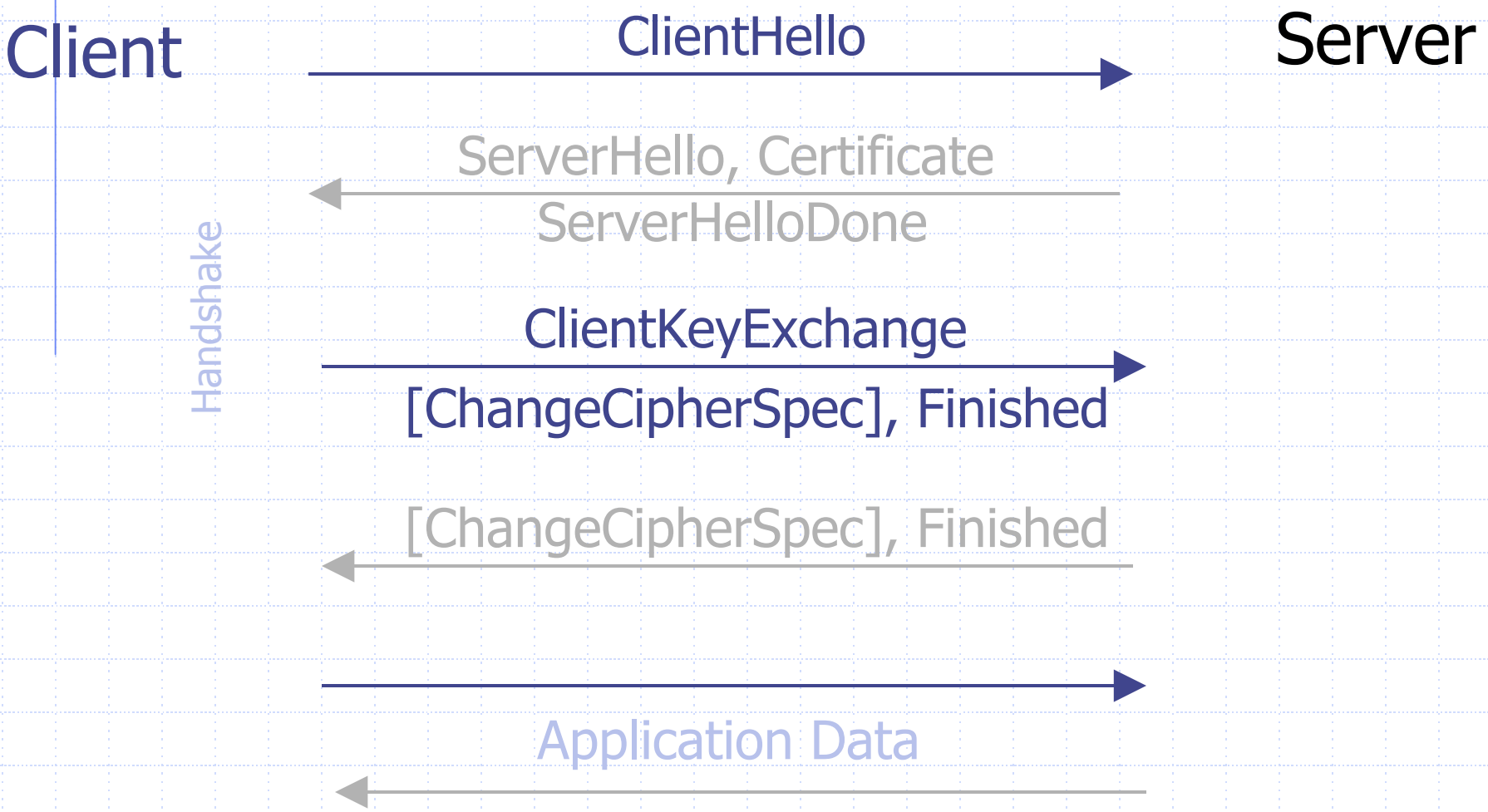
Datagram Transport Layer Security (DTLS)

Eric Rescorla

IETF 60 PMTUD Meeting

TLS Protocol Overview



DTLS Protocol Overview

- Datagram-capable version of TLS
- Protocol flow same as TLS
  - Initial handshake (2-3 round trips)
  - Data sent in DTLS records
- Provide reliability for handshake phase
  - Using standard timeout and retransmits

PMTU Issues

- Handshake phase
  - Certificate message can be quite large
    - 500-1000 bytes per certificate
    - Can this exceed PMTU?
  - Compromise between PMTU discovery and handshake completeness
- Application data transfer
  - Records can be up to 2^{14} bytes
  - Obviously this exceeds most PMTUs