Secondary Certificates

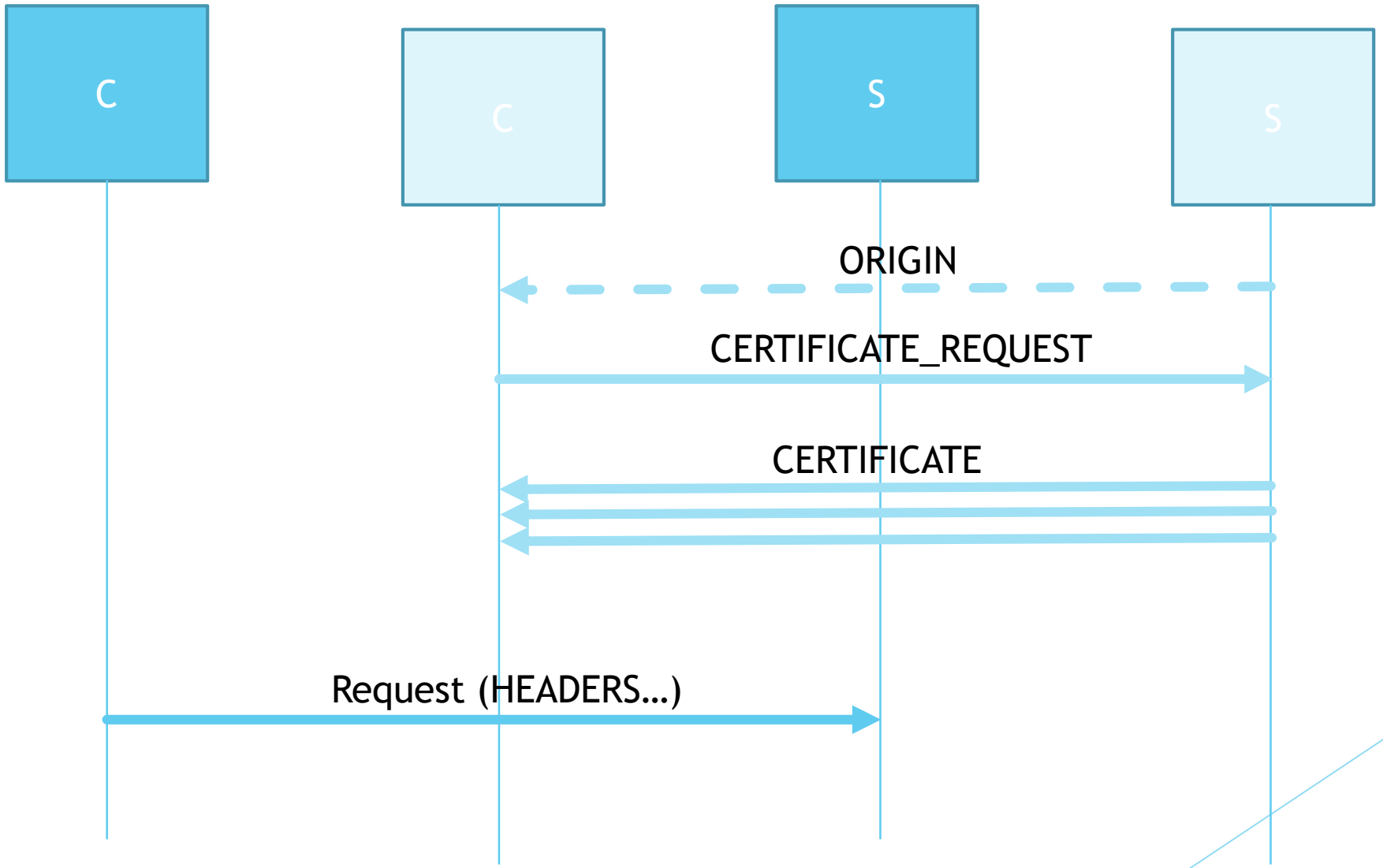
TLS has a limitation….

HTTP/2 makes it worse….

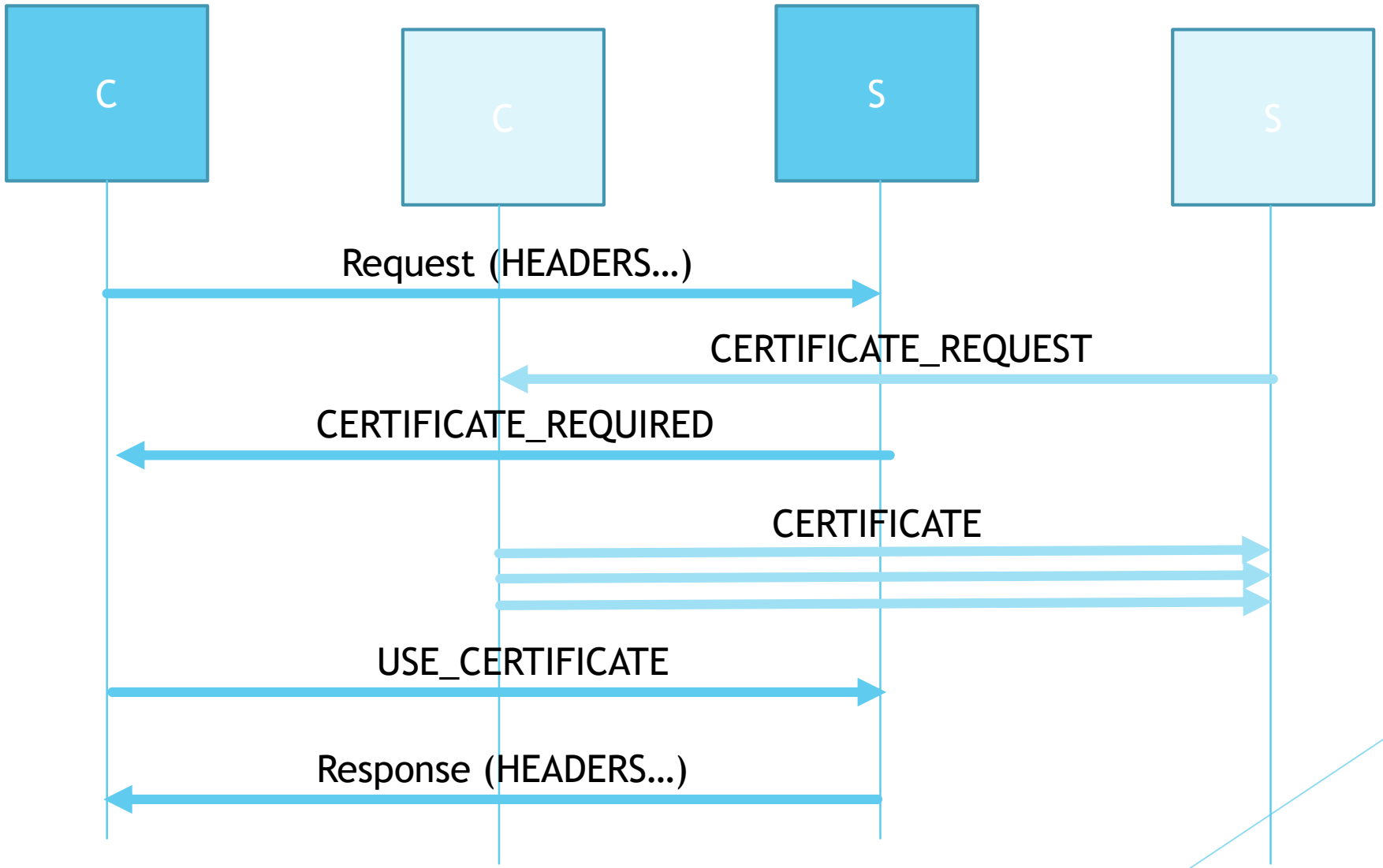
Recap: Several new frames

- CERTIFICATE_REQUEST (Stream 0)
  - Describes a certificate the sender would like to see
  - Modeled on TLS 1.3 CertificateRequest message
    - Contains list of Extensions (SNI, OID filters, issuing CAs, etc.)
  - Probably being replaced with an Exported Authenticator Request
- CERTIFICATE_REQUIRED (Stream N)
  - References a CERTIFICATE_REQUEST, indicates request will not proceed until that request is fulfilled (or a certificate is selected)
- CERTIFICATE (Stream 0)
  - Contains an Exported Authenticator (draft-ietf-tls-exported-authenticator)
  - Bound to TLS channel, results in a certificate chain
- USE_CERTIFICATE (Stream N)
  - Optionally permits stream-by-stream selection of which certificate to use

Server Certificates



Client Certificates



Possible advantages

- For servers:
  - Not everyone has (or wants) a monolithic certificate
  - Better coalescing
    - Often good for performance
    - Single CDN has many authoritative names it serves
  - Potential option for encrypted SNI
    - Connect to a well-known name/cert
    - Include request for “actual” desired certificate after SETTINGS frame
- For clients:
  - Client certificates are a real thing
  - Able to selectively present certificates per request, if you care
    - …and ability not to, if you don’t

What's new?

- Uses TLS Exported Authenticators – no more crypto at the "wrong" layer
  - Adopted by TLS WG in Chicago
- Still need to tighten up some of the crypto properties
  - Likely leads to some changes in the Exported Authenticators draft

- **Ready for adoption?**