Secondary Server Certificates

Moving Certificates to the HTTP/2 Framing Layer

- Martin, just now: HTTP/2 frames for presenting certificate chain and proof of private key possession
- Could we use the same frames to present certificates in the opposite direction?

Possible advantages

- More flexible certificate management
  - Servers can maintain distinct certificates for different sets of names
  - Easier to replace one without others (see: ACME)
- 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

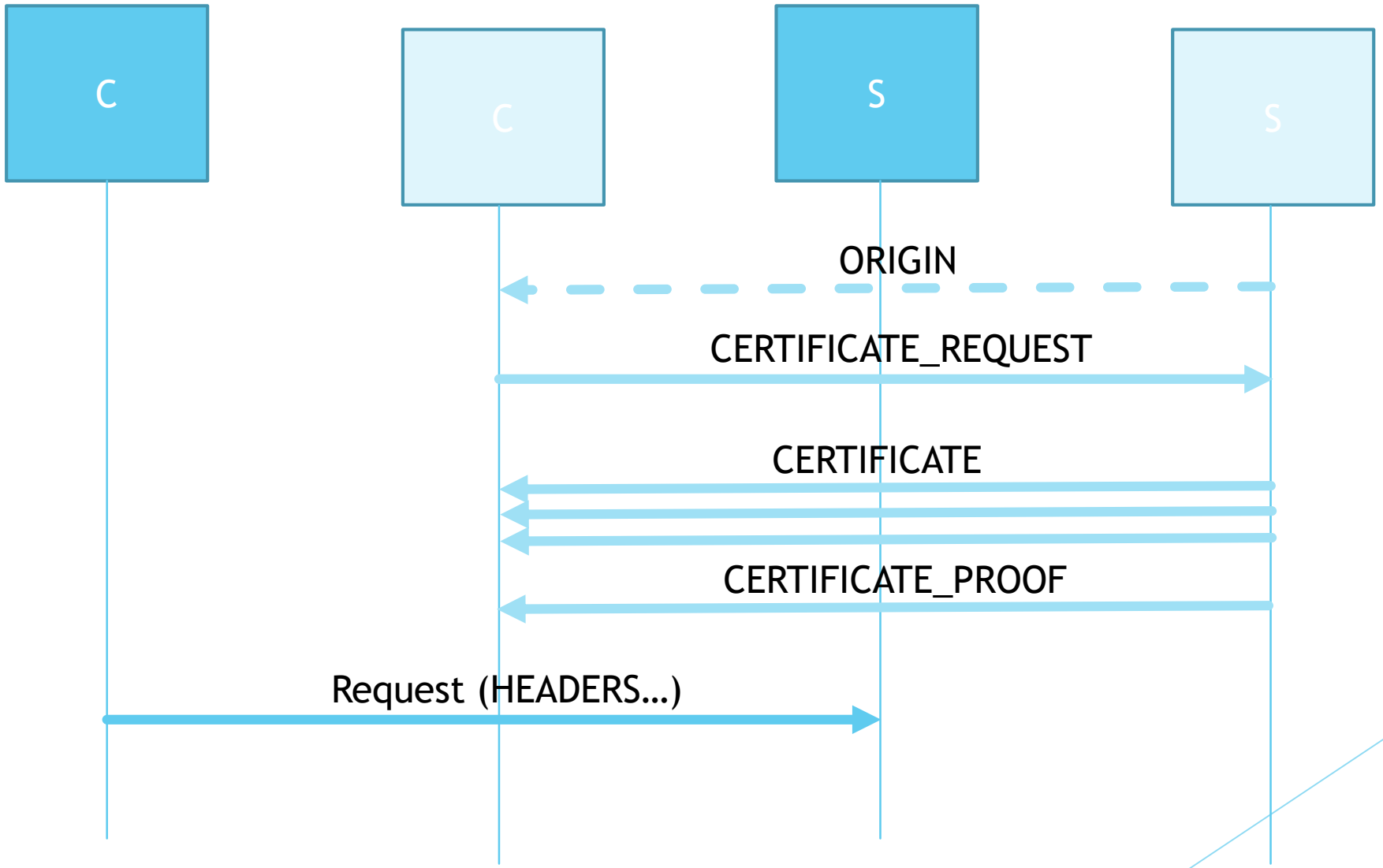
Possible disadvantages

- *See Eric's talk on Monday about ways coalescing can go wrong*
- Certificate handling in the HTTP layer
  - "We do this all the time! What could go wrong?"
- Duplicated code for certificate management
  - True with client certs as well – duplicative code in
- Second attack vector for cert spoofing

Changes needed to client cert model

- Reverse direction
  - Client sends challenges, server sends certificates
  - Client cert explicitly omits the reverse direction rather than prohibiting it
- Properties in request
  - Server sends client a list of allowed cert issuers
  - Client wants to send server a single desired end-entity name
- Stream binding
  - Client certs start/end on-stream (CERTIFICATE_REQUIRED, USE_CERTIFICATE)
  - Server certs typically need to be requested before request is made
    - Exception: Cross-domain server push?

Flow


C
C
S
S
ORIGIN
CERTIFICATE_REQUEST
CERTIFICATE
CERTIFICATE_PROOF
Request (HEADERS...)