

H2

# CLIENT CERTS



# PROBLEM

WE'VE DONE THIS BEFORE

HTTP/2 prevents servers from using client certificate authentication

except in narrow cases

HTTP requires reactive client authentication

# ABORTIVE ATTEMPTS

...

Use renegotiation in TLS 1.2/spontaneous auth in TLS 1.3

Microsoft have a proprietary setting for renegotiation

Hard to correlate certificates (and requests for same) with request

Confused deputy problem

Solution: hoist all the machinery into HTTP/2

# CERTIFICATE PROOFS

## CERTIFICATE TABLE

CERTIFICATE\_REQUEST (from server)

=> CERTIFICATE\* + CERTIFICATE\_PROOF (from client)

Substantially similar to TLS CertificateRequest, Certificate, CertificateVerify

Uses a TLS exporter to get the signature input

All happens on stream 0

Allows certificates to be added to the connection and later referenced many times (up to 256 certs, that is)

# REQUEST BINDING

## TABLE LOOKUP

A server can indicate that it wants a certificate to complete a request

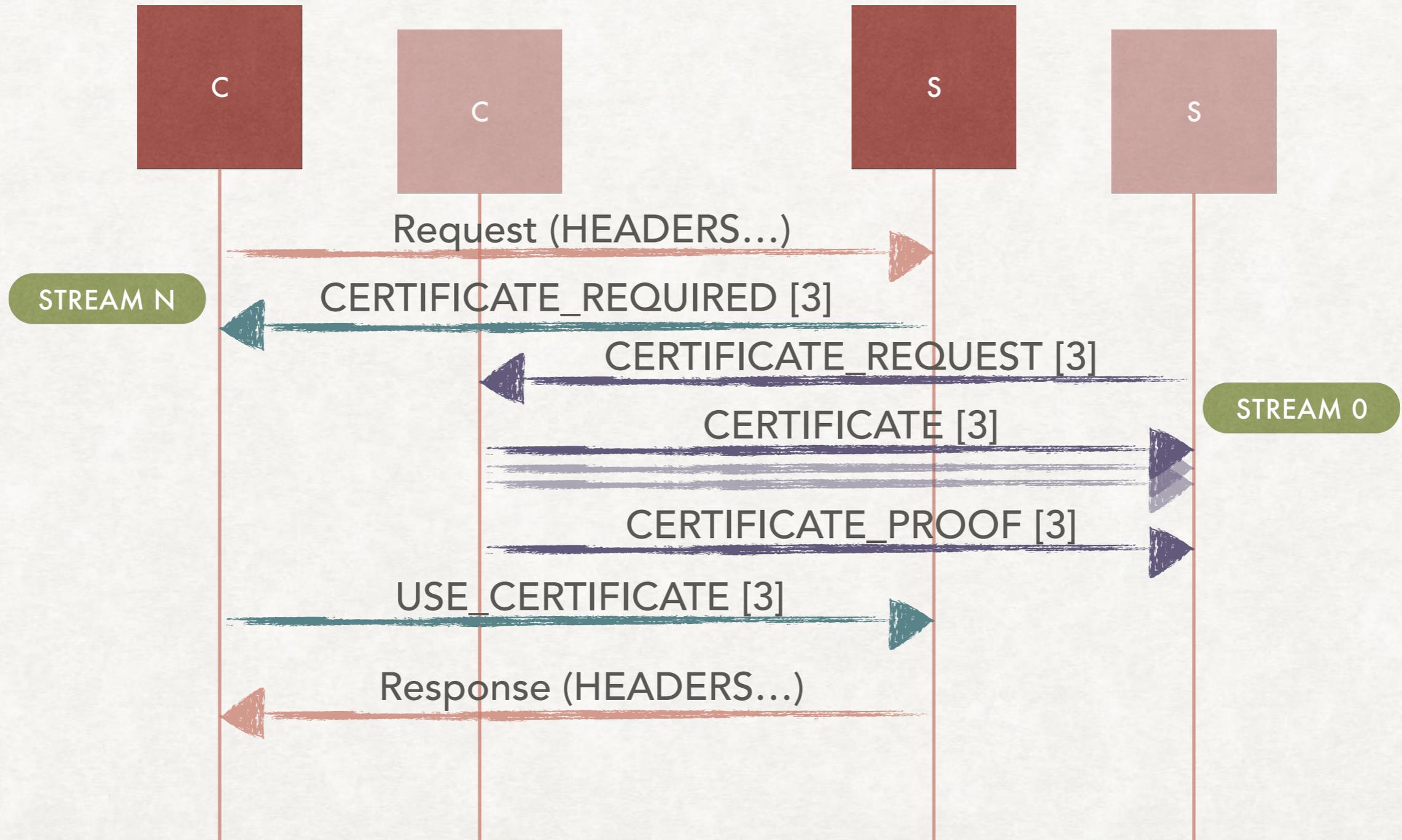
CERTIFICATE\_REQUIRED

A client indicates that it wants to use a certificate

USE\_CERTIFICATE

An empty frame indicates that the request is denied

# FLOW EXAMPLE



...

# NEXT STEPS

