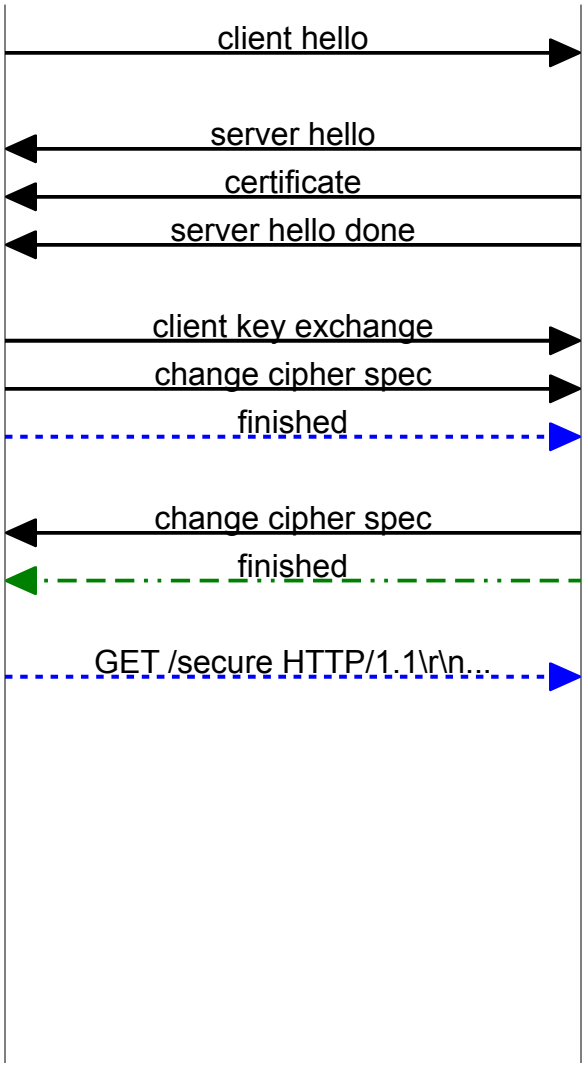
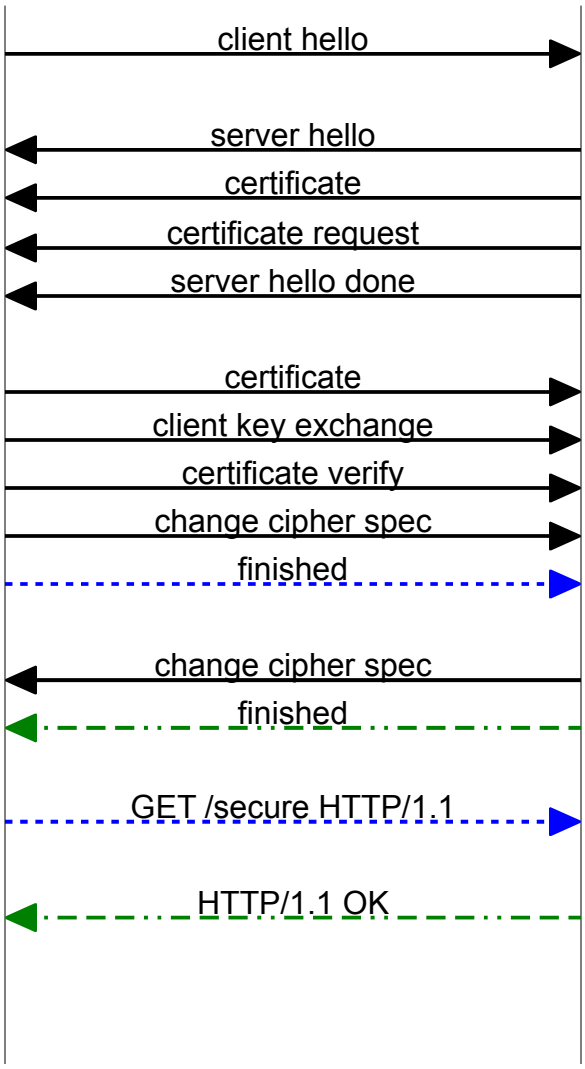
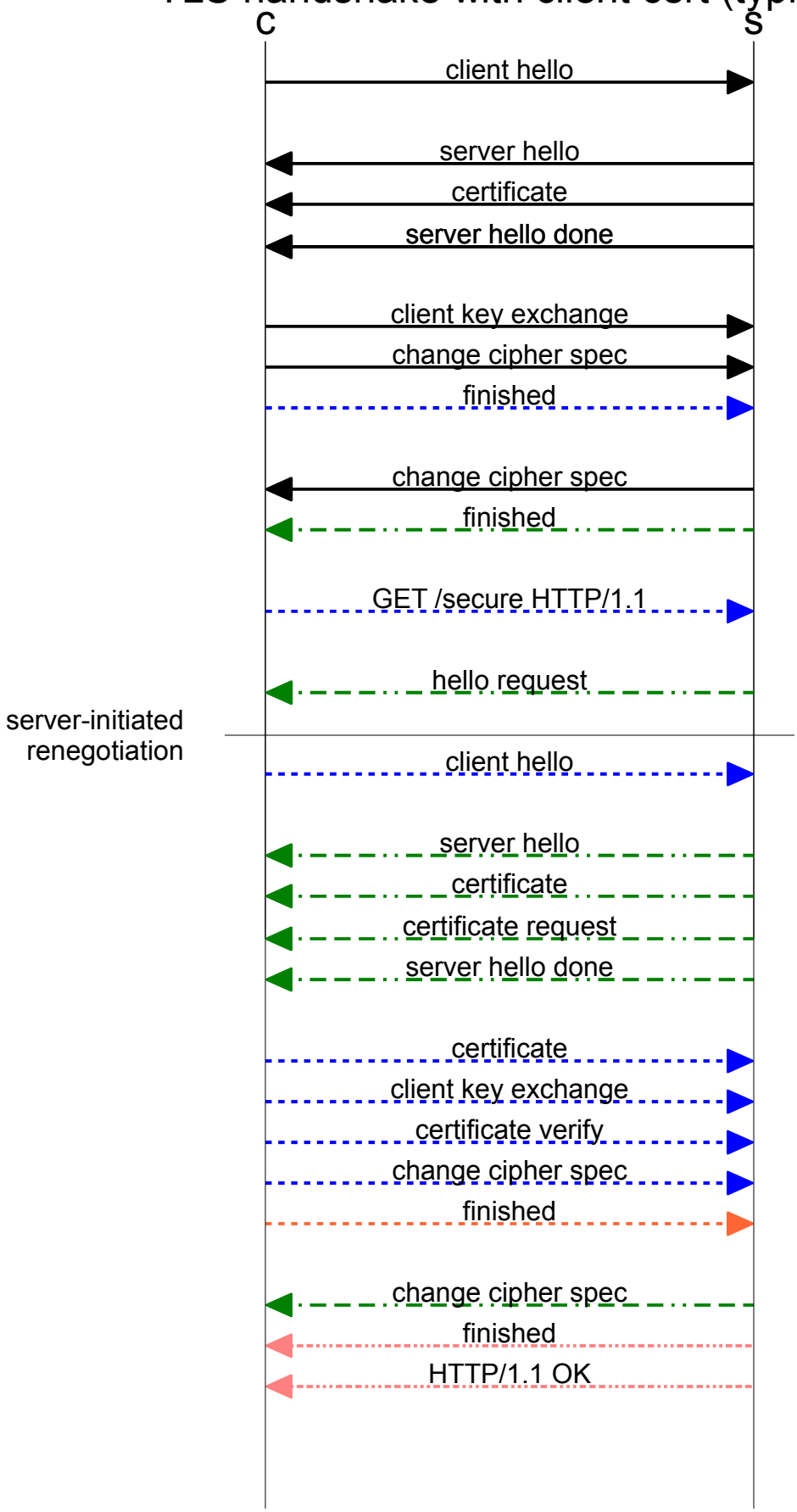
basic TLS handshake

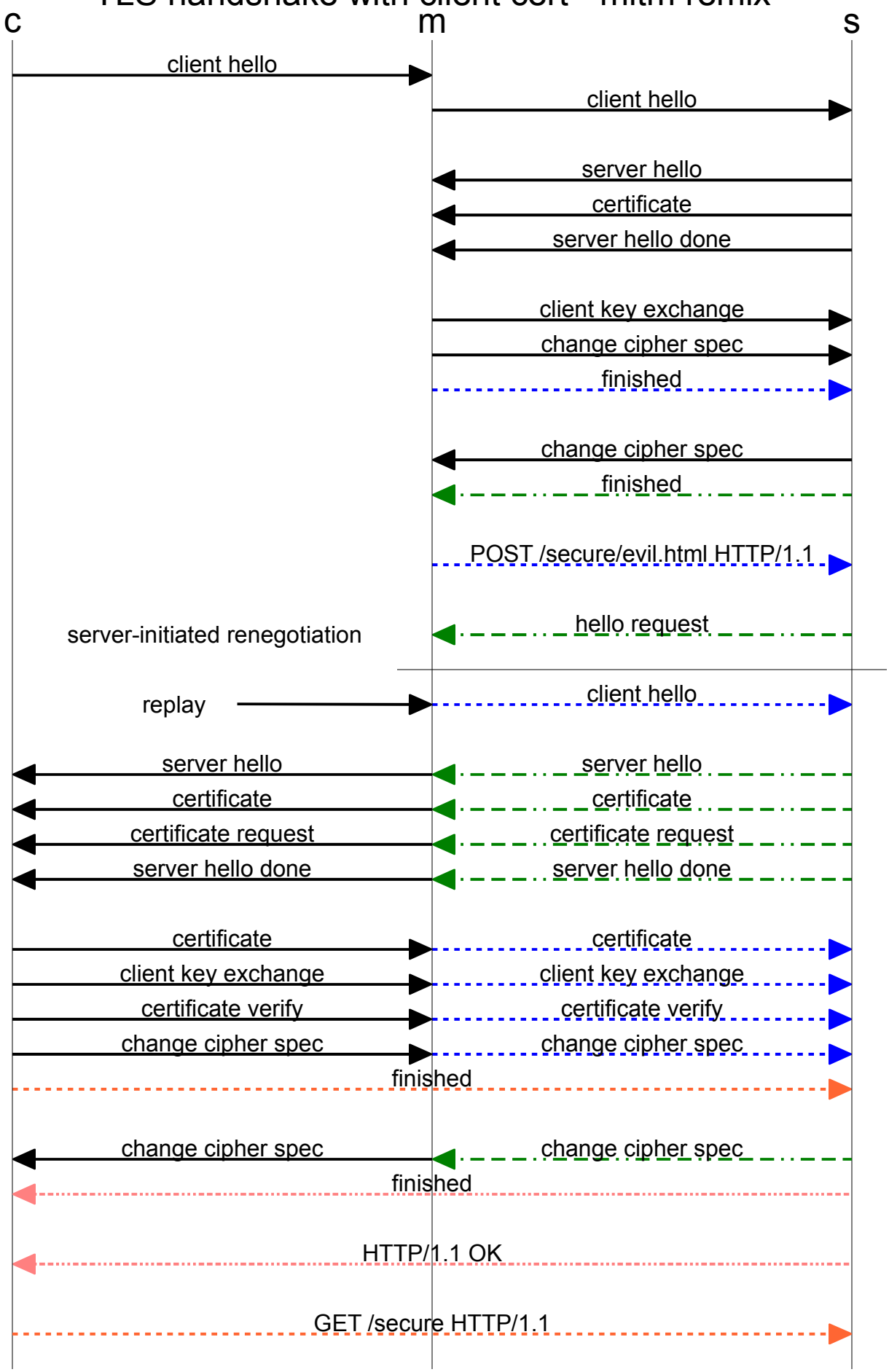


TLS handshake with client cert (ideal)



TLS handshake with client cert (typical)




TLS handshake with client cert - mitm remix
c
m
s
client hello
client hello
server hello
certificate
server hello done
client key exchange
change cipher spec
finished
change cipher spec
finished
POST /secure/evil.html HTTP/1.1
server-initiated renegotiation
hello request
replay
client hello
server hello
certificate
certificate request
server hello done
server hello
certificate
certificate request
server hello done
certificate
client key exchange
certificate verify
change cipher spec
finished
certificate
client key exchange
certificate verify
change cipher spec
change cipher spec
finished
HTTP/1.1 OK
GET /secure HTTP/1.1