

## SSL Time-Diagram

### Main Scenario with Client's Certificate and Session Resumption

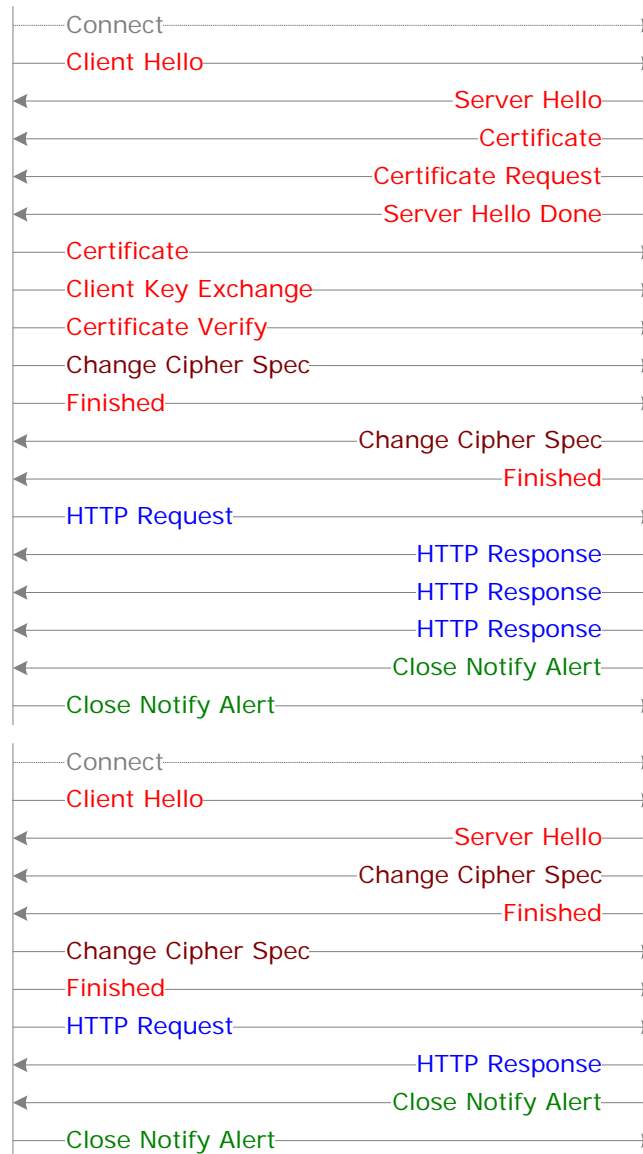
V1.0 – March 2, 2005

This document provides a detailed description of the sequence of exchanges between an SSL Client and an SSL Server. This main scenario includes the Client's Certificate option, as well as the Session's resumption.

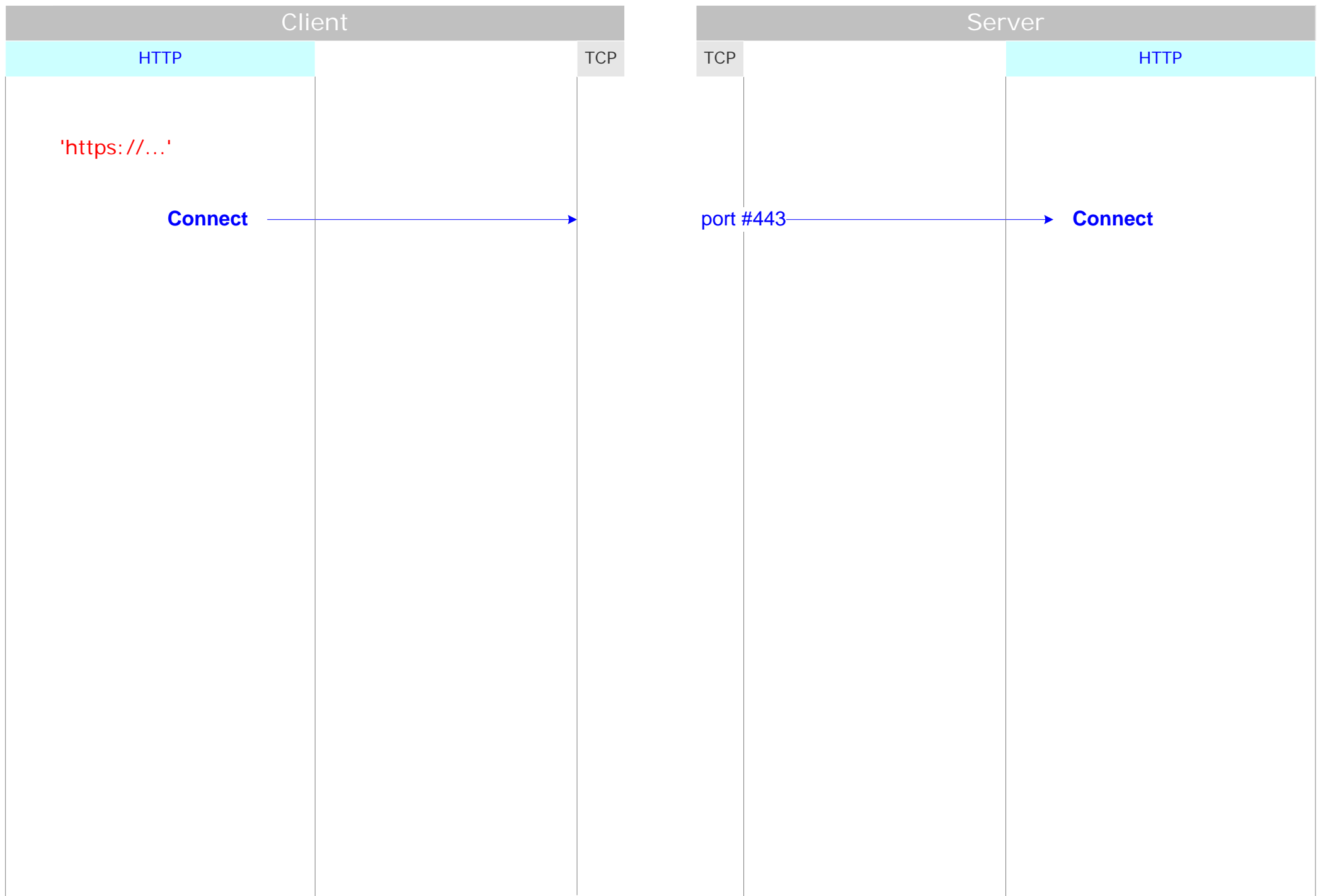
The type of encryption algorithm used with this case study is "stream cipher".

This document is supplemented by two other documents describing variants related to the first exchanges.

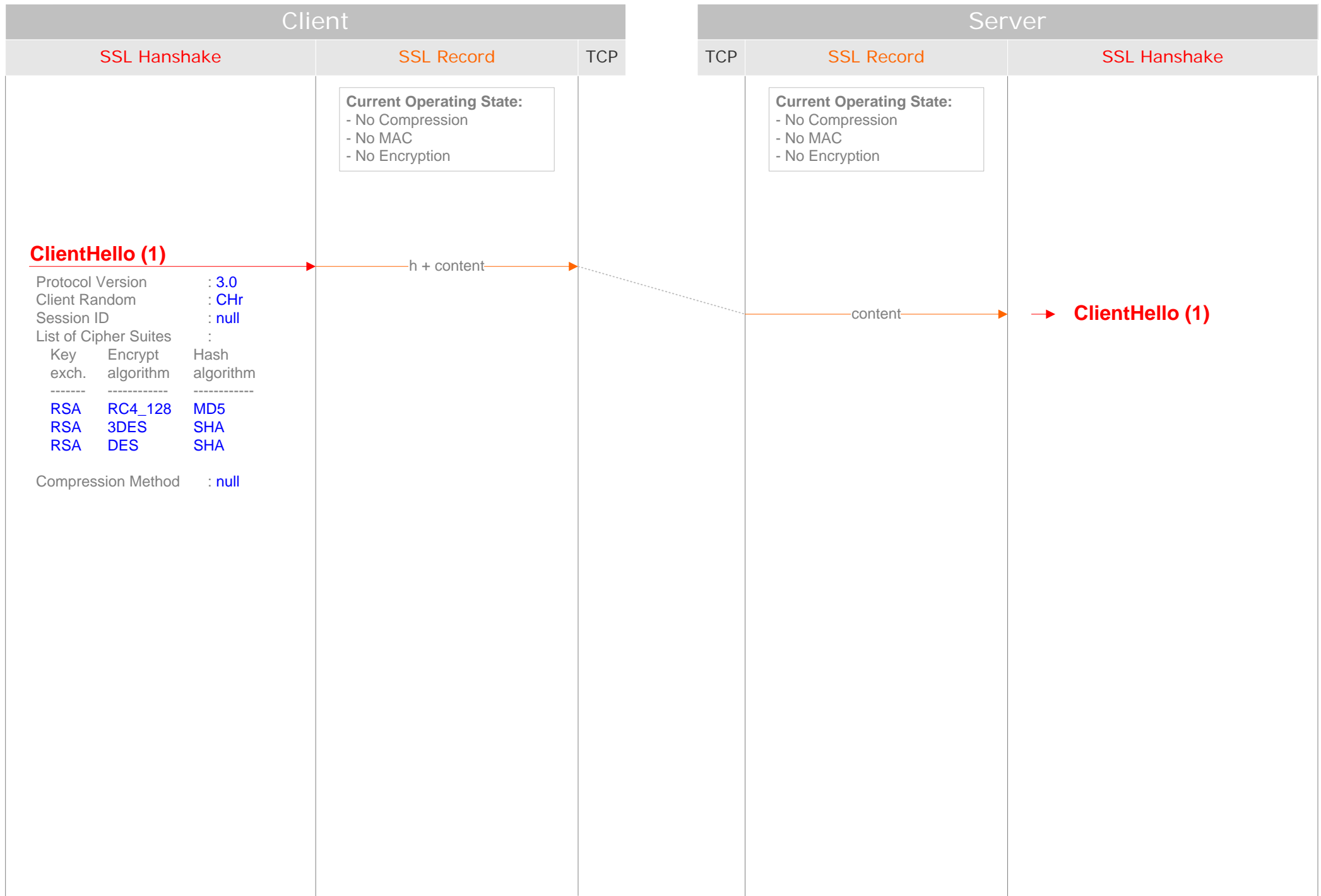
# Summary of Exchanges



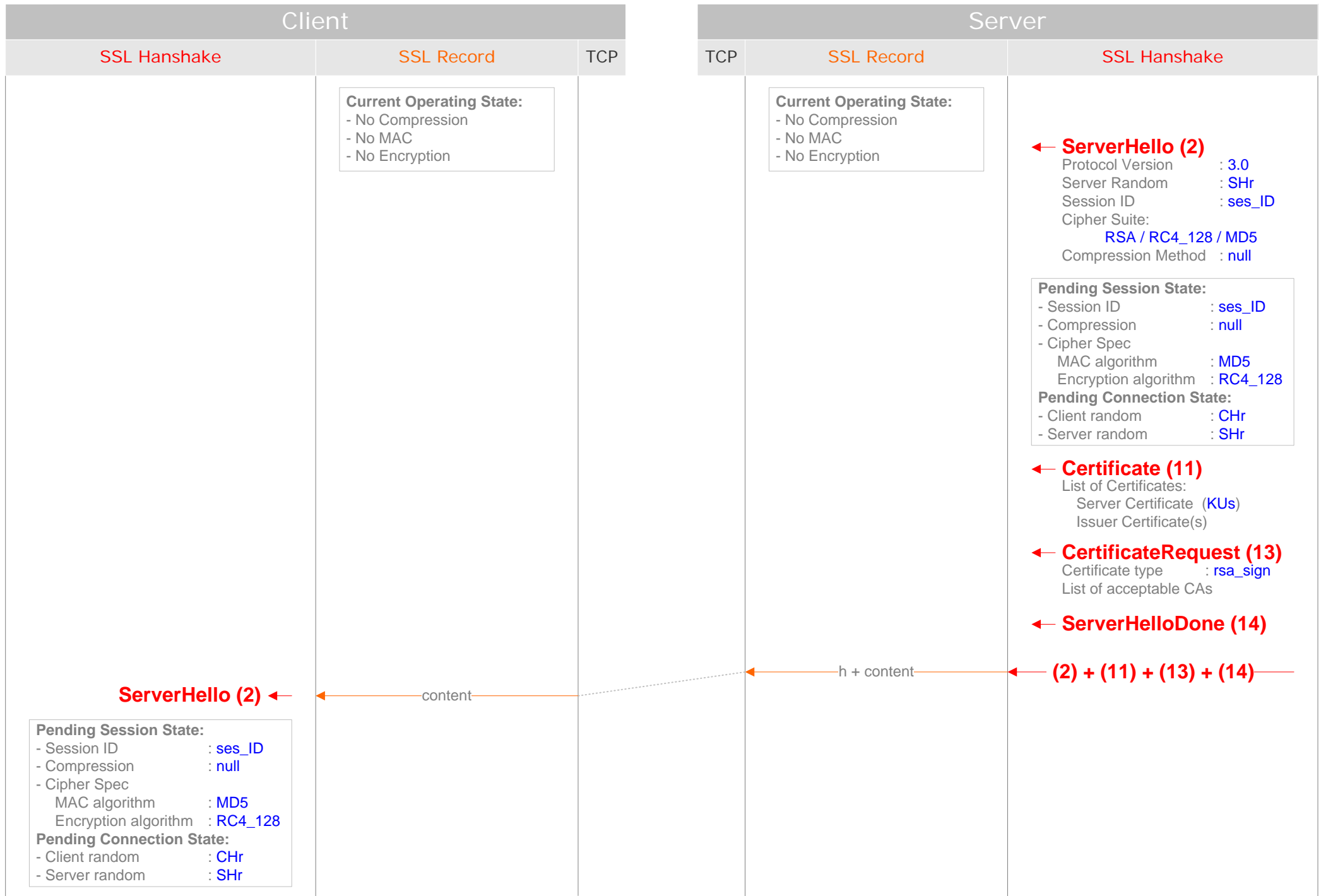
# (1) First TCP Connection



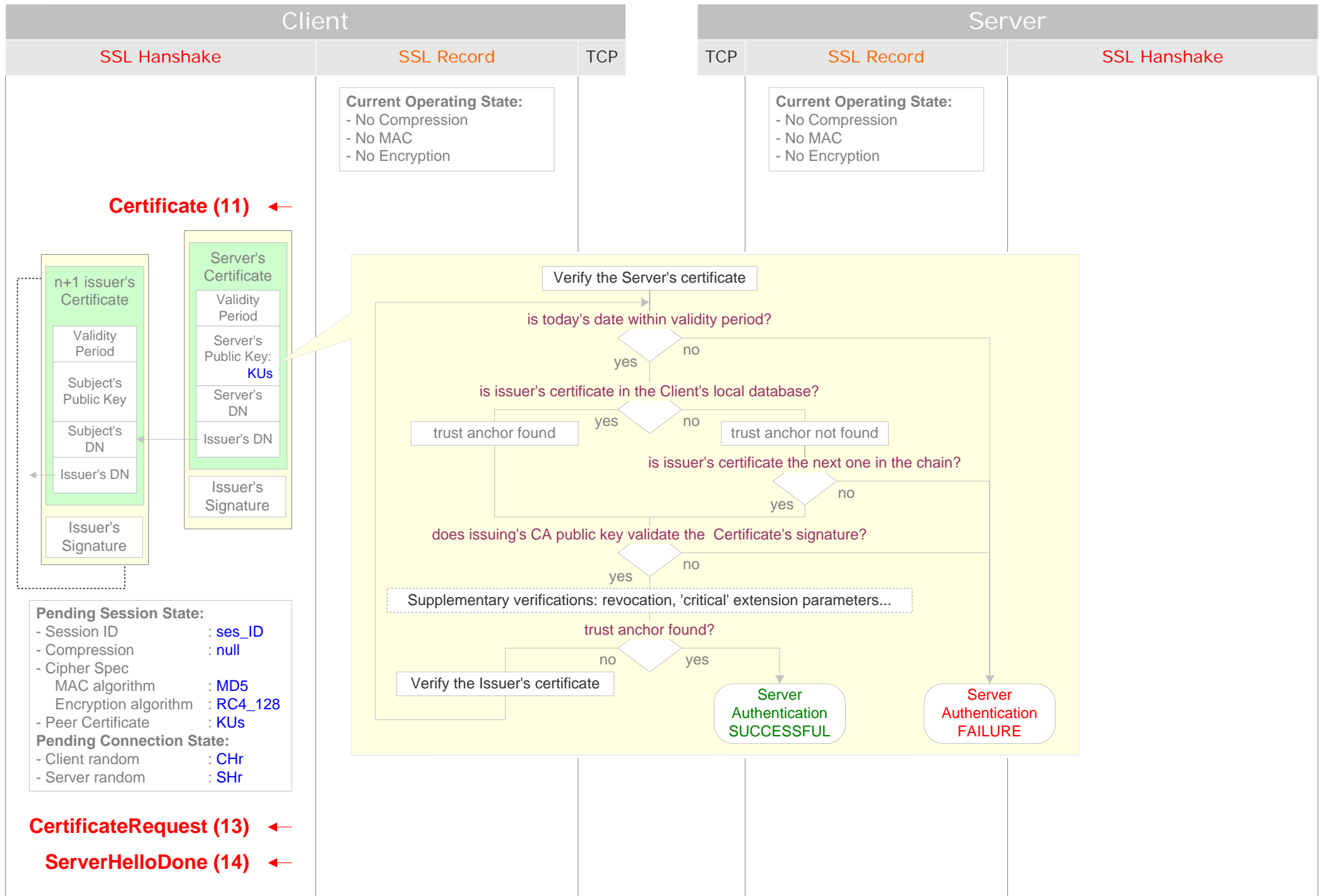
## (2) Client Hello



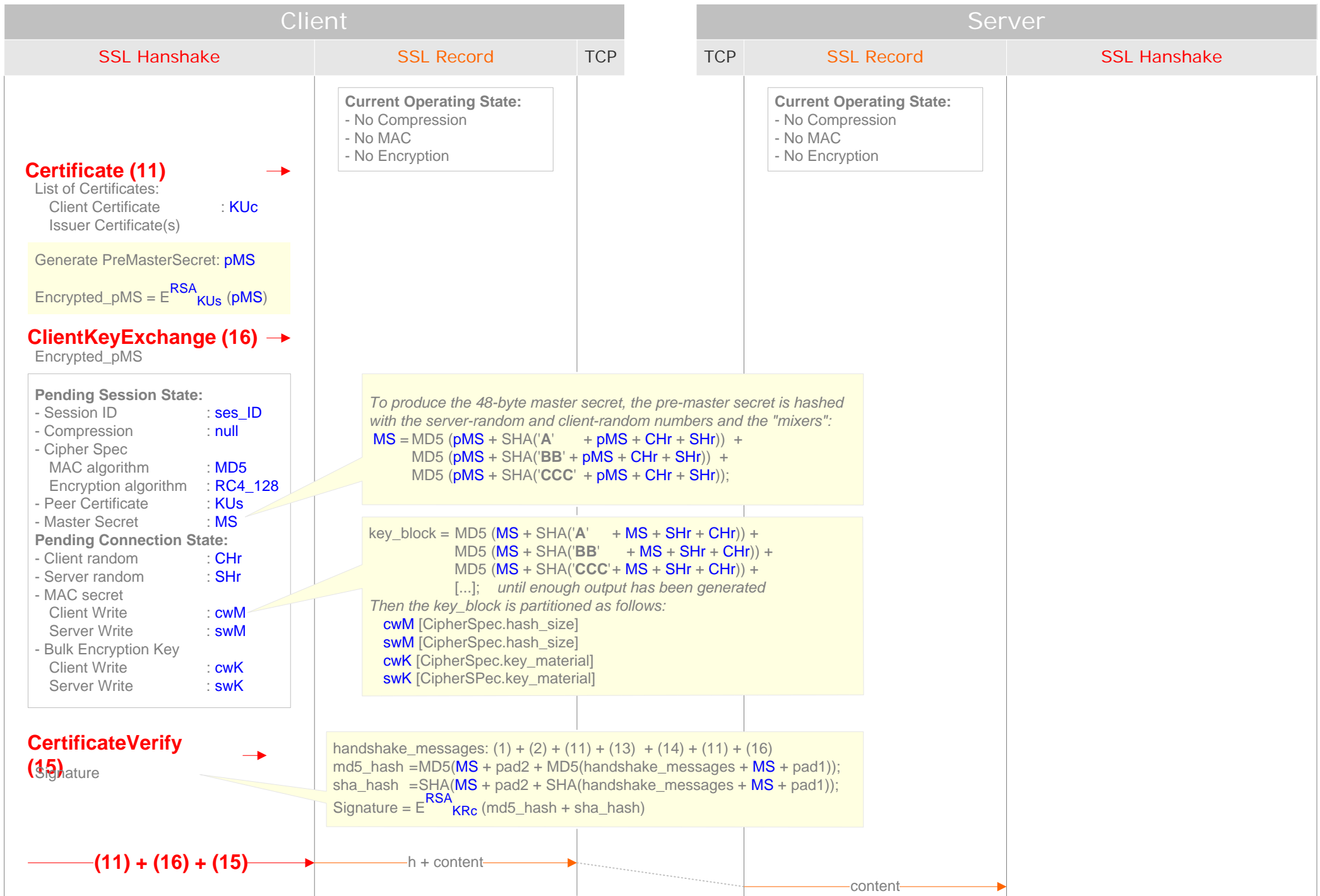
### (3) Server Hello



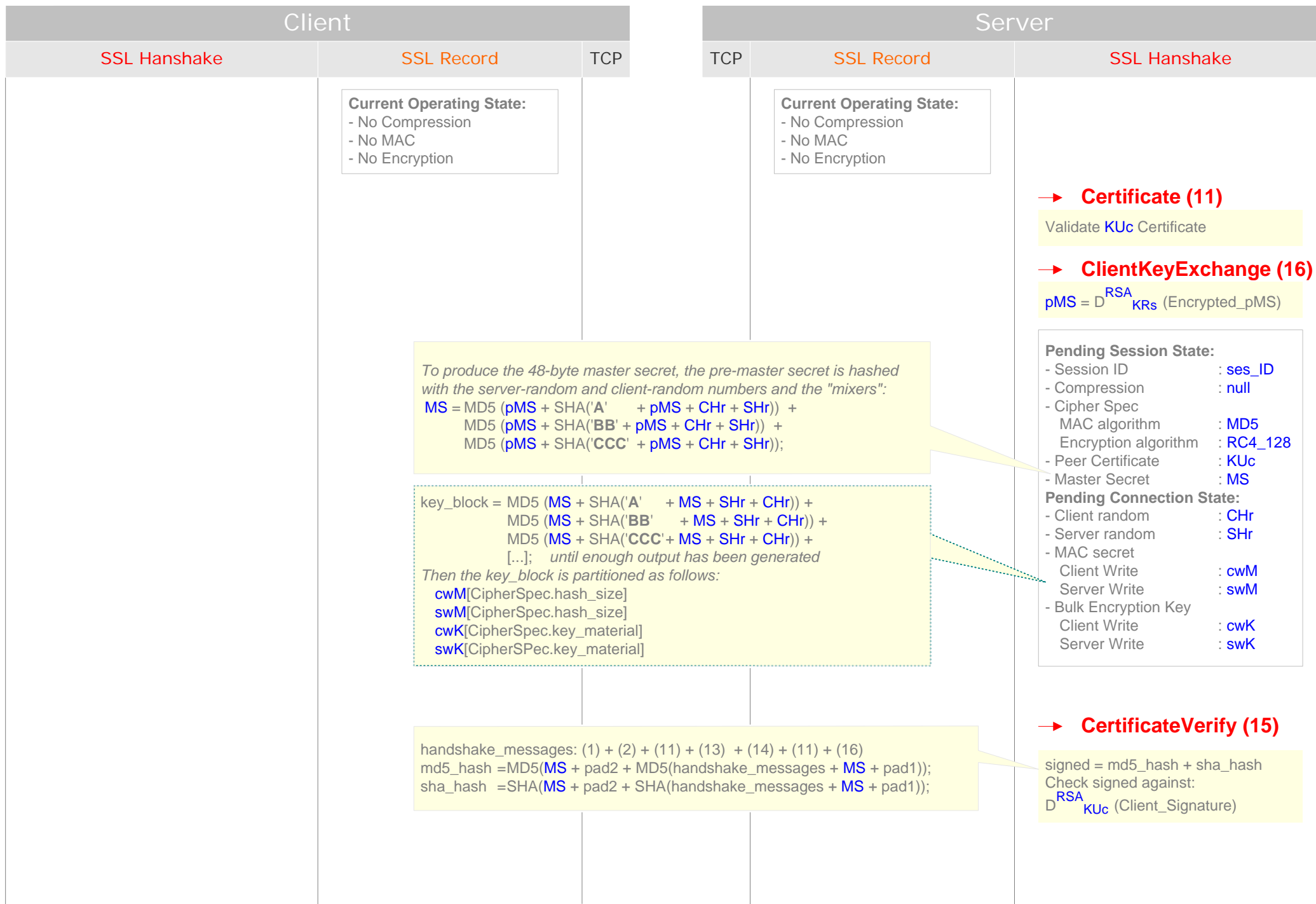
## (4) Server Authentication



## (5) Client Certificate & Key Exchange (Send)

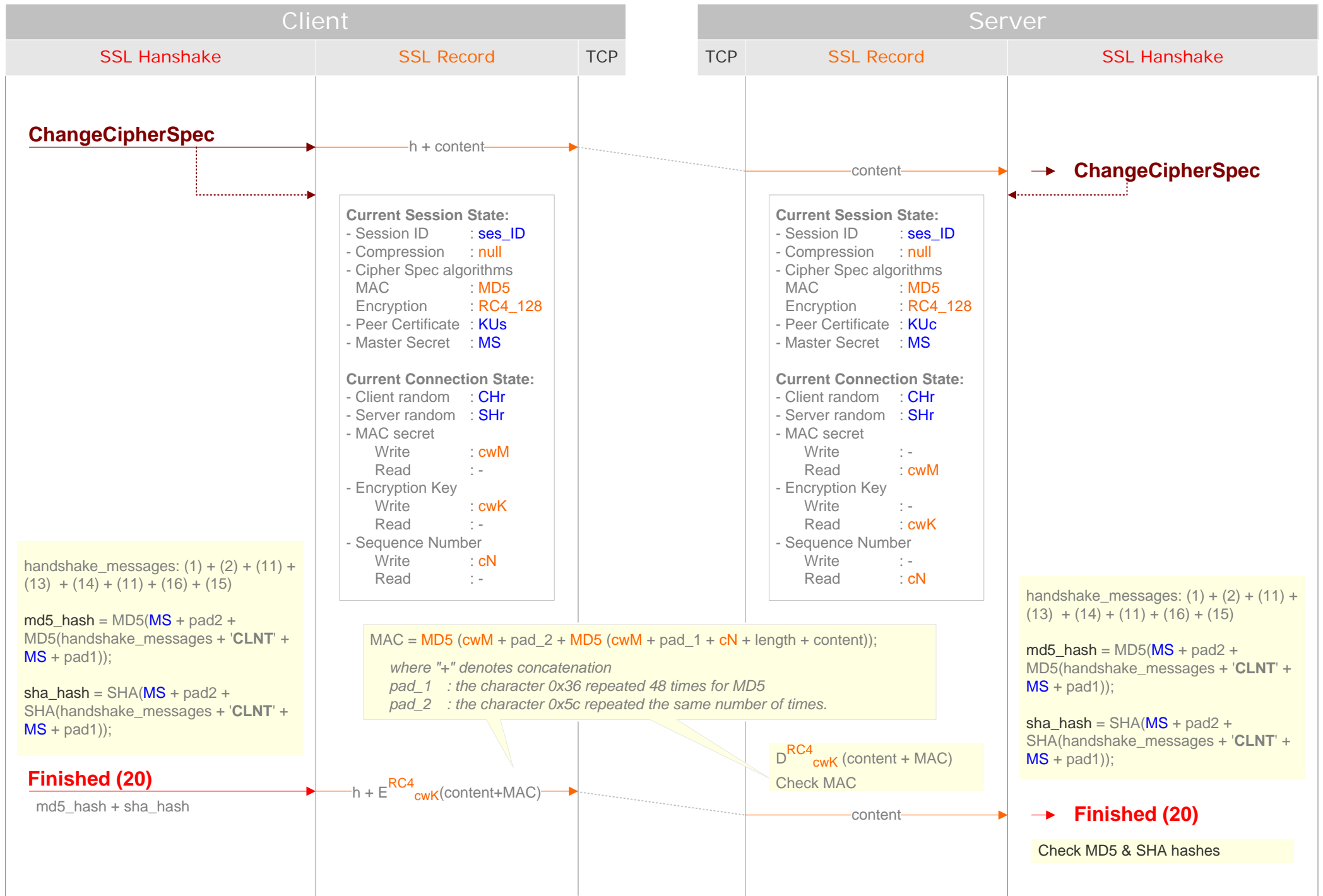


## (6) Client Certificate & Key Exchange (Receive)

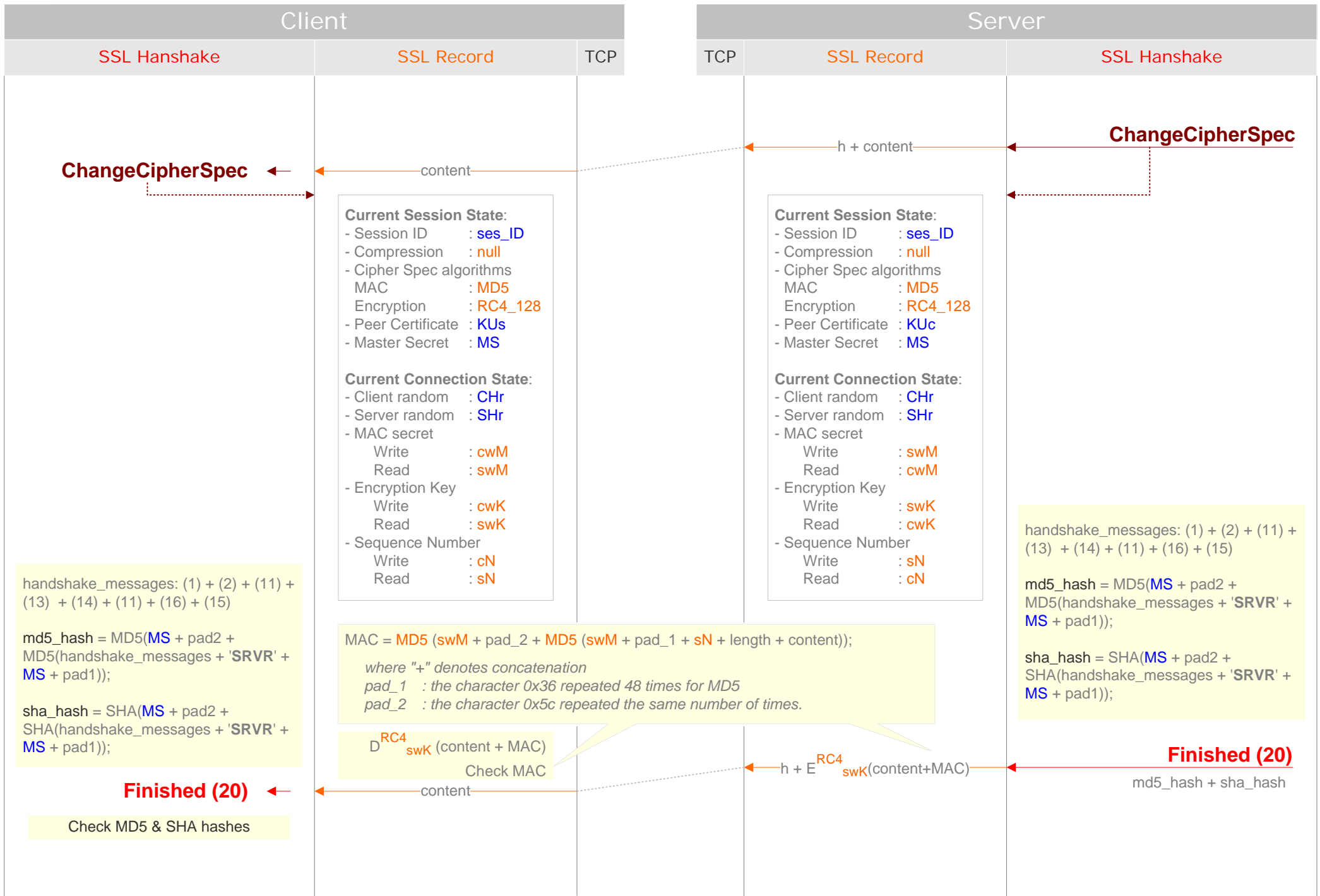




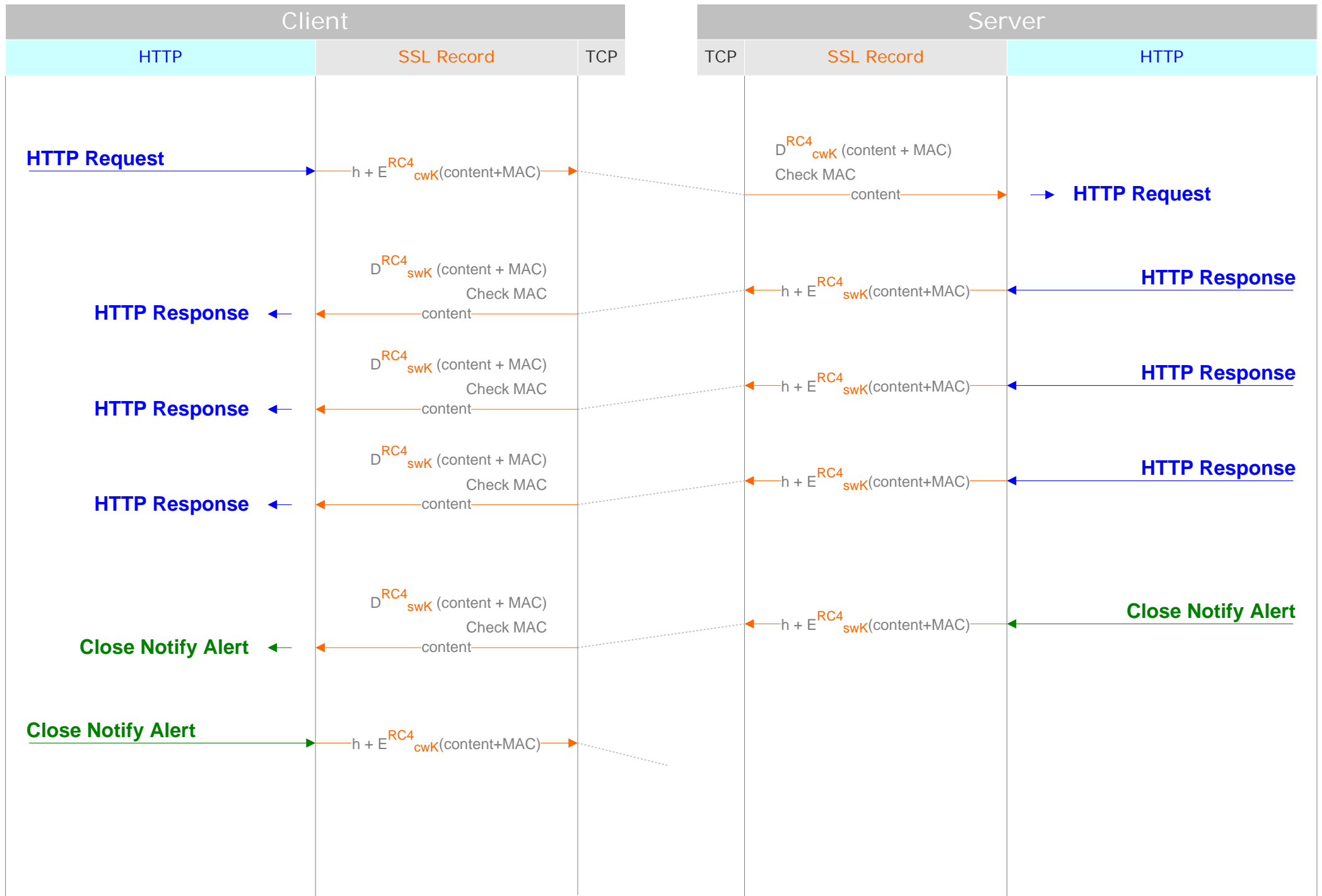
# (7) Client Change Cipher Spec & Finished



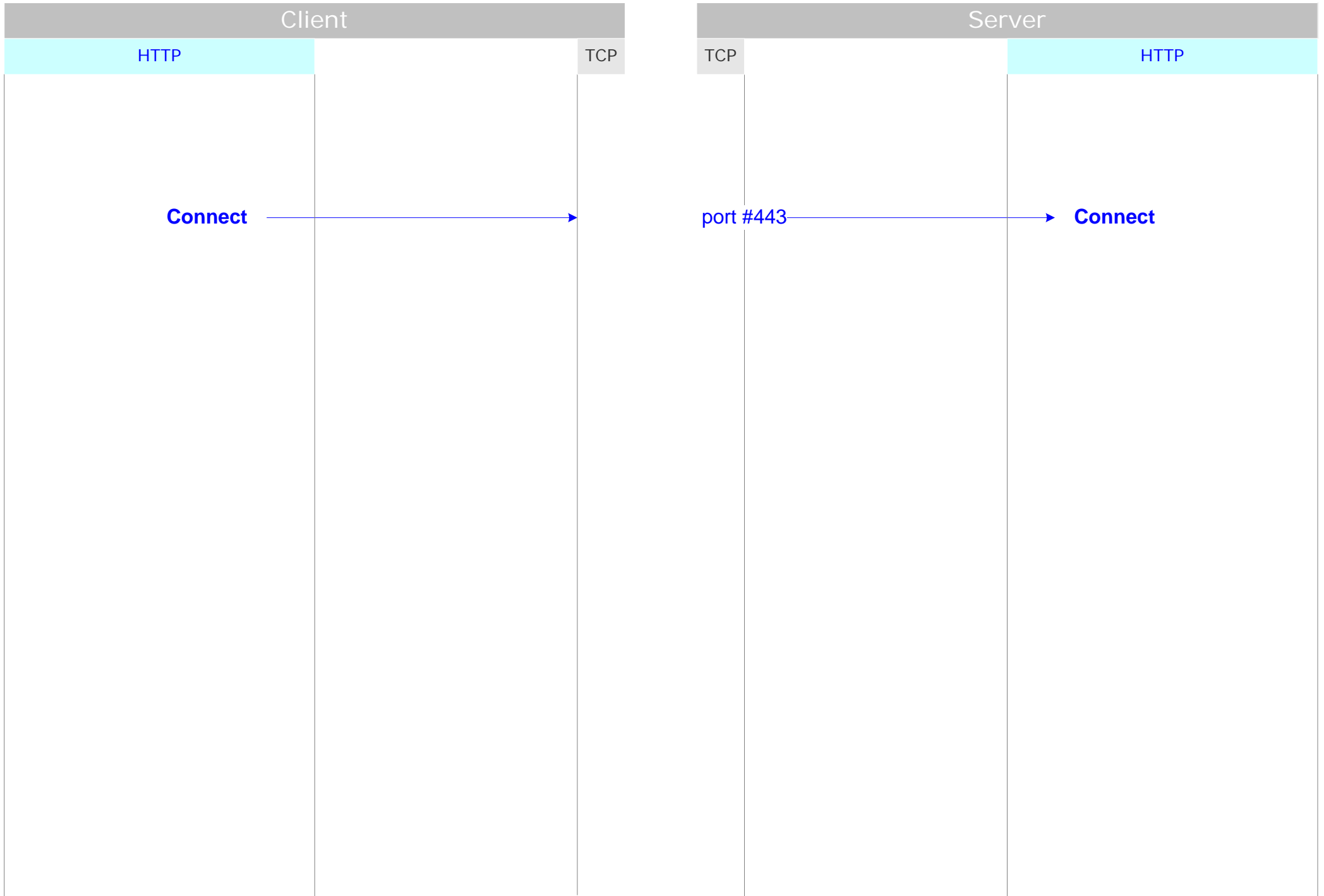
## (8) Server Change Cipher Spec & Finished



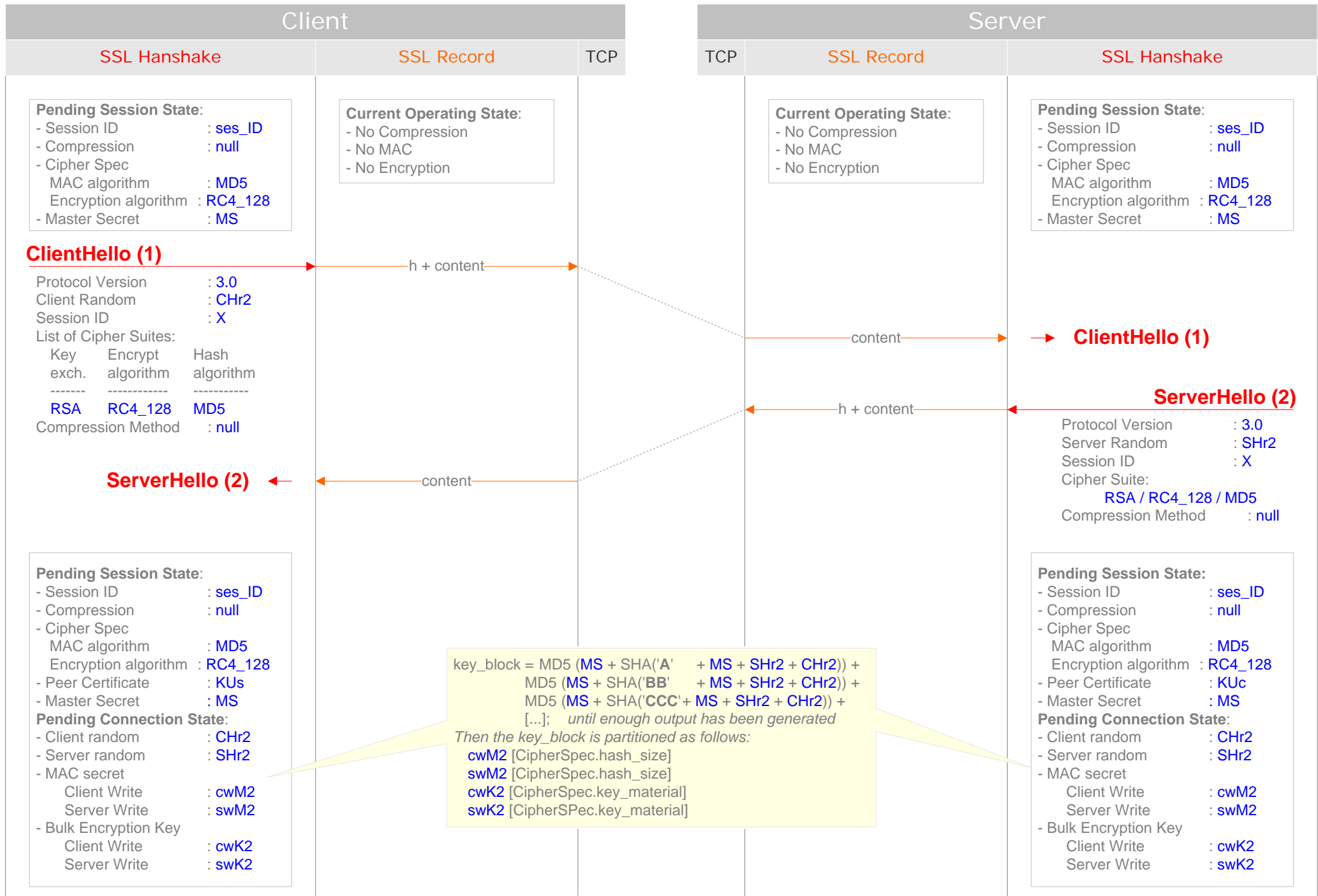
# (9) HTTP Exchanges & Close Notify Alert



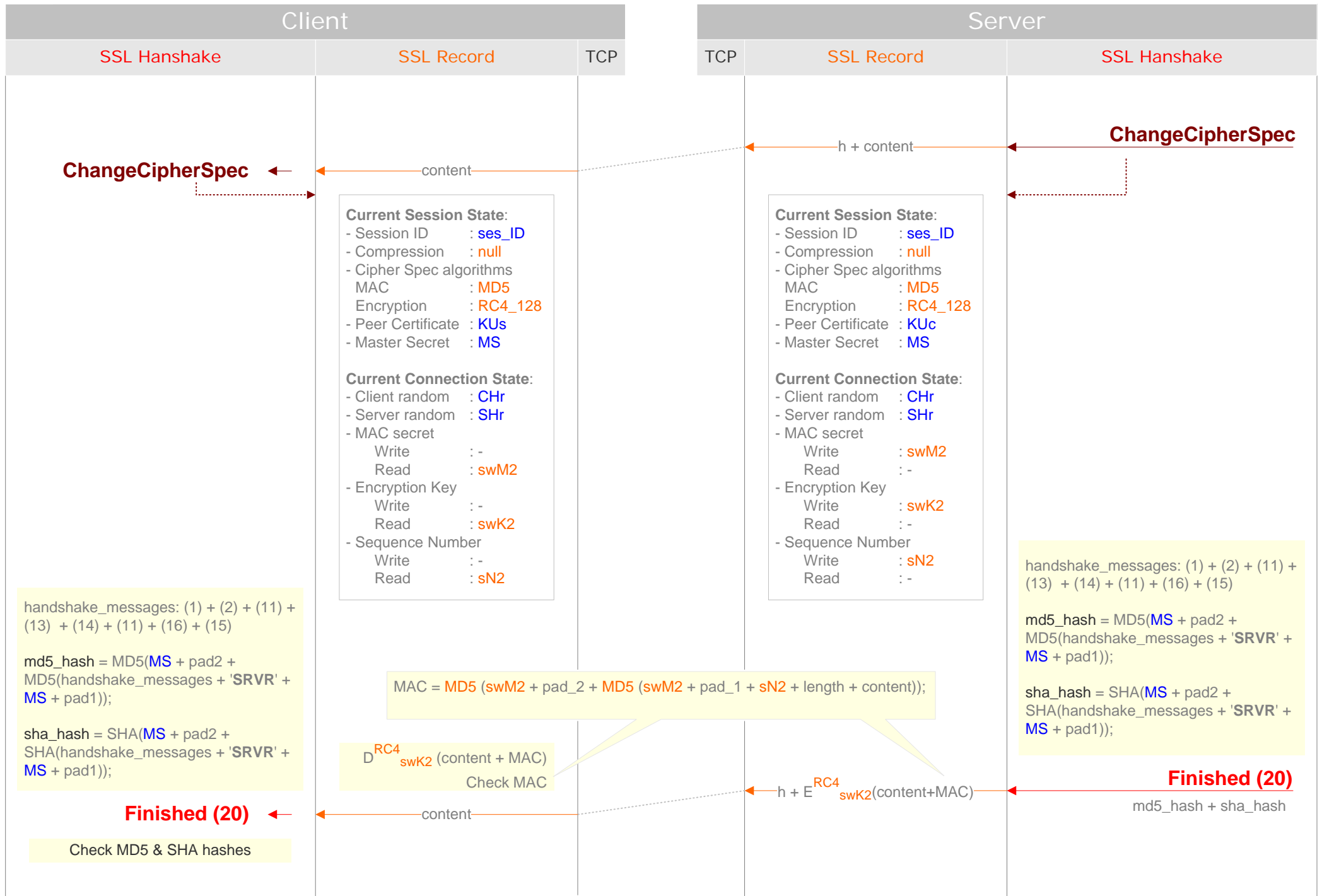
## (10) Second TCP Connection



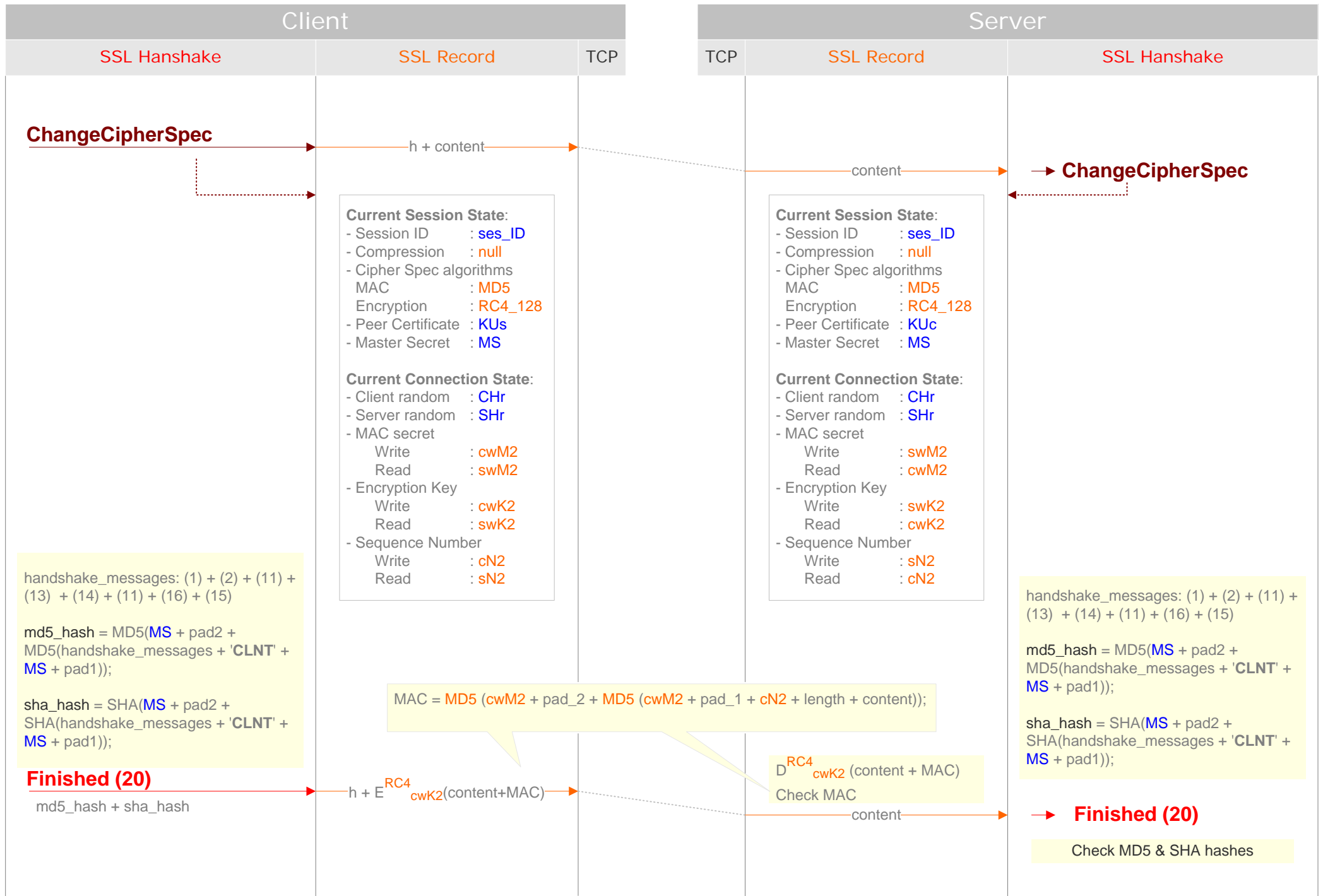
# (11) Client & Server Hello's – Session Resumption



# (12) Resumption: Server Change Cipher Spec & Finished



# (13) Resumption: Client Change Cipher Spec & Finished



# (end) HTTP Exchanges & Close Notify Alert

