50.005 – Programming Assignment 2

Secure File Transfer

Team Members:  
Ashlyn Goh Er Xuan 1002840 Cl02  
Wong Chi Seng 1002853 Cl02

# Instructions to Run

## Prerequisite:

Java is required

## For CP-1:

In CP1Server.java, change the following:  
- private key file path (.der file)  
- server certificate file path (.crt file)

In CP1Client.java, change the following:  
- server’s IP address (use “localhost” if running both on the same computer)  
- CACSE.crt file path (CA’s certificate)  
- Name of the file to be transferred  
- Path of the file to be transferred

Run CP1Server.java before running CP1Client.java. If file transfer has been successful, the file will be transferred to the server and saved to the same directory.

## For CP-2:

Do the same as above, except with CP2Server.java and CP2Client.java

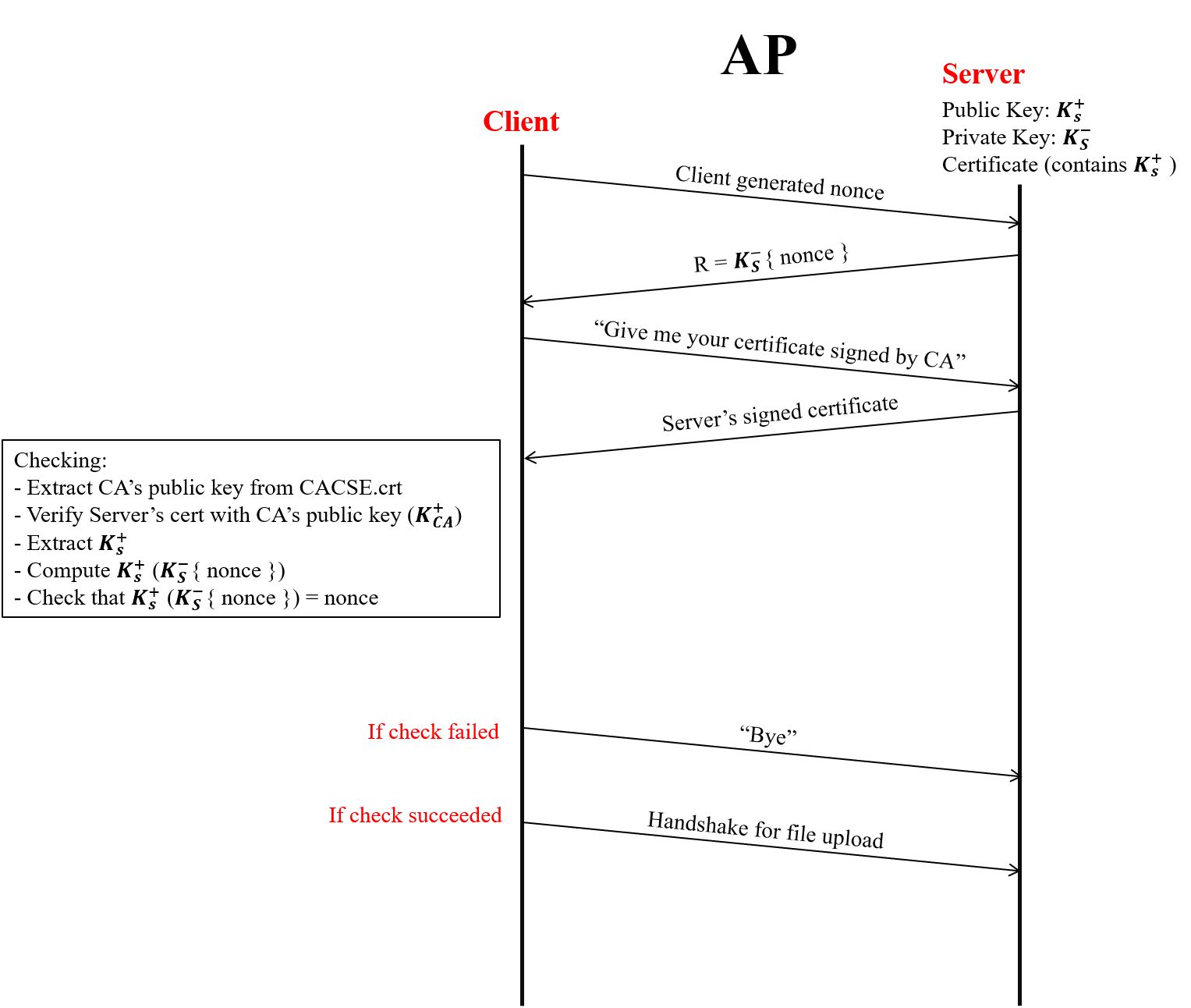
# Problem with Original Protocol

The problem with the original protocol is that it does not prevent a playback attack. Hence, an attacker can maliciously repeat a valid data transmission. In our case, the attacker can store information without authorisation and then retransmit it back to the client to trick the client into transferring the file.

To prevent the playback attack, we introduced a nonce into our protocol. The client generates a nonce and sends it to the server. On the other hand, the server must return the nonce that is encrypted with its private key back to the client. Thereafter, the client would check if the decrypted nonce (with server’s public key) matches the original nonce sent. More details are included in the specification diagram in the next section.

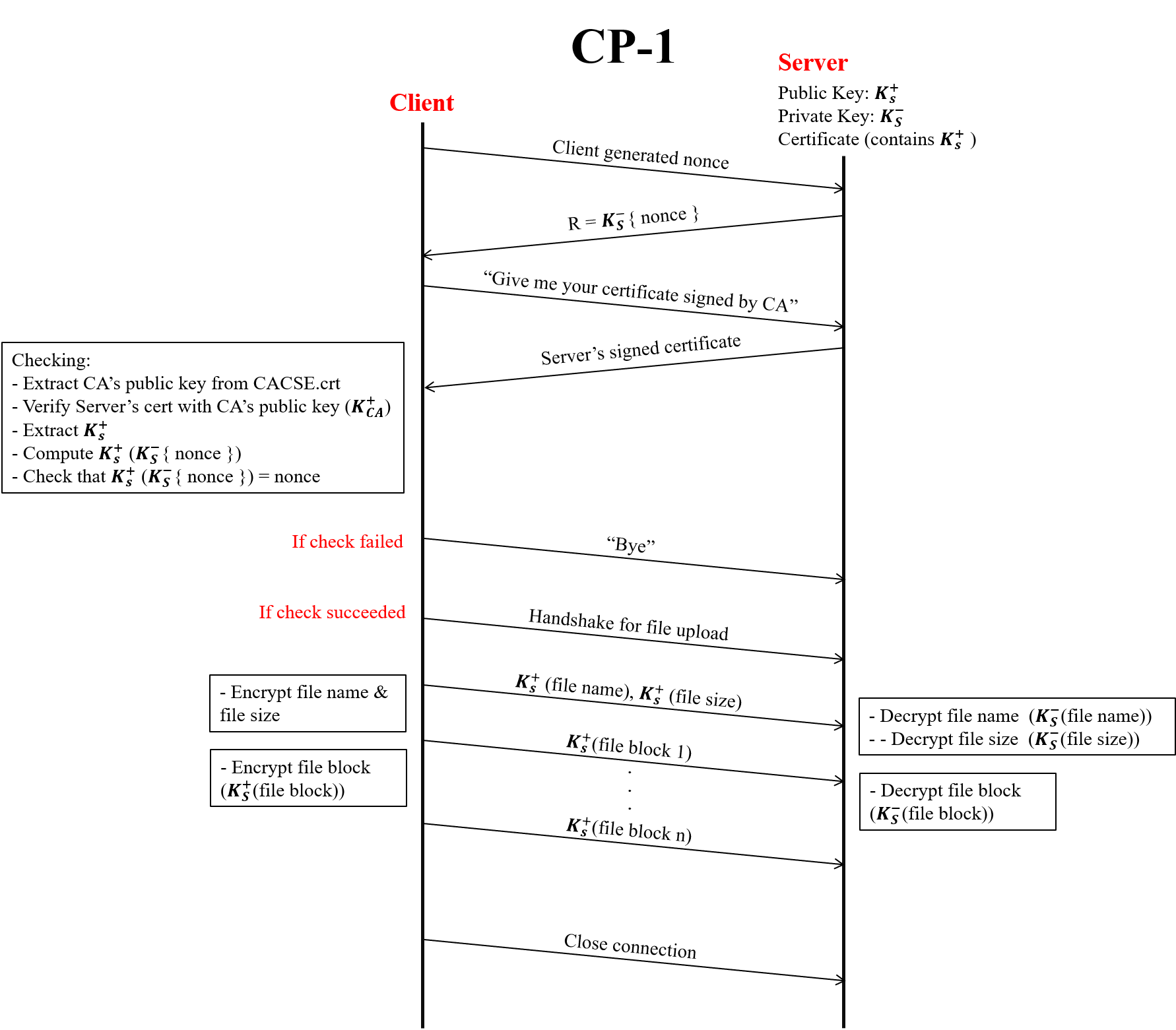
# Protocol Specifications

## AP Protocol



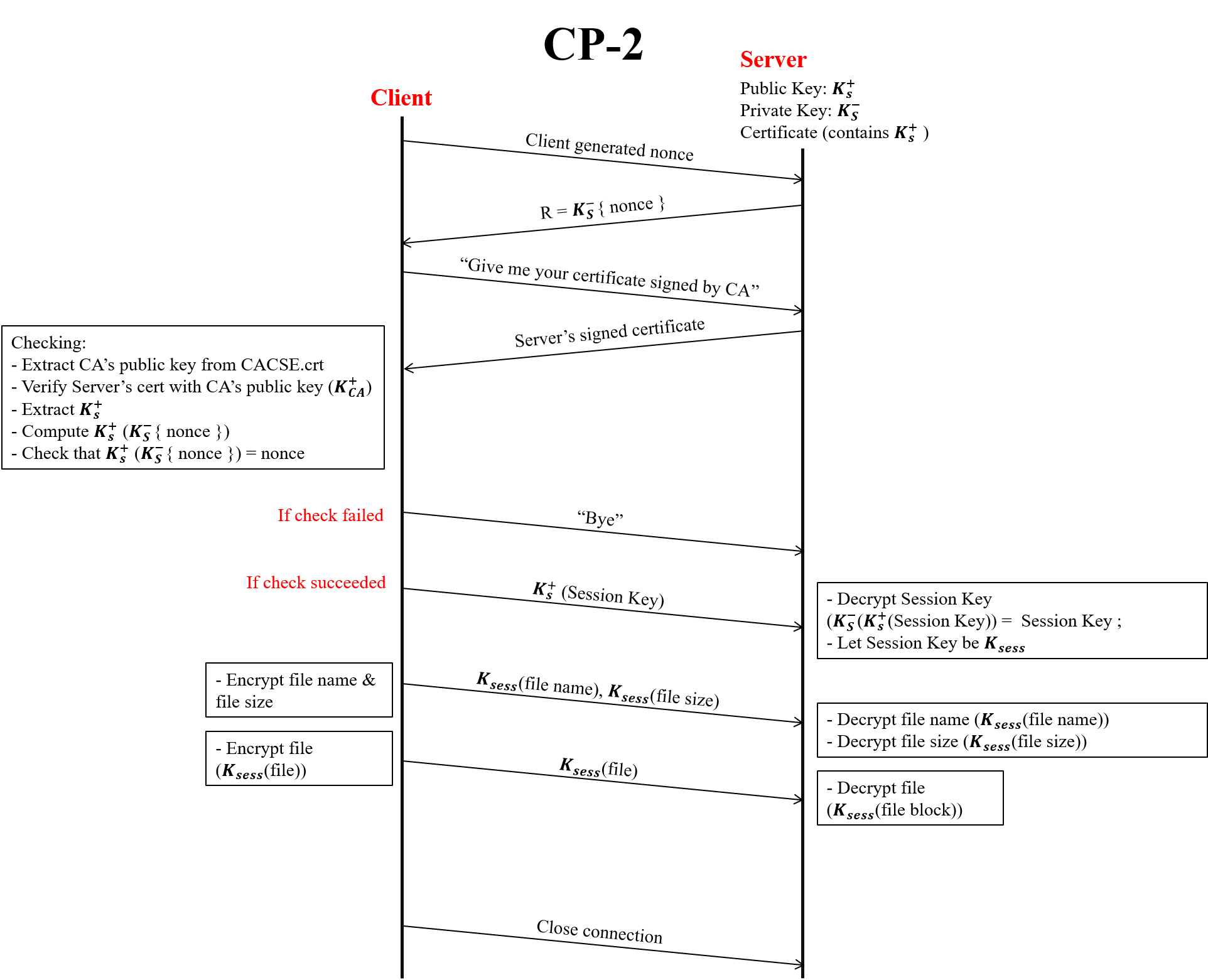
*Figure 1: Authentication Protocol Specification*

## CP-1 Protocol



*Figure 2: CP-1 Specification*

## CP-2 Protocol



*Figure 3: CP-2 Specification*

# Results

## Table

|  |  |  |
| --- | --- | --- |
| **Protocol** | **File Size (KB)** | **Time Taken (ms)** |
| CP-1 |  |  |
|  |  |
|  |  |
|  |  |
|  |  |
| CP-2 |  |  |
|  |  |
|  |  |
|  |  |
|  |  |

## Plot

# Conclusion