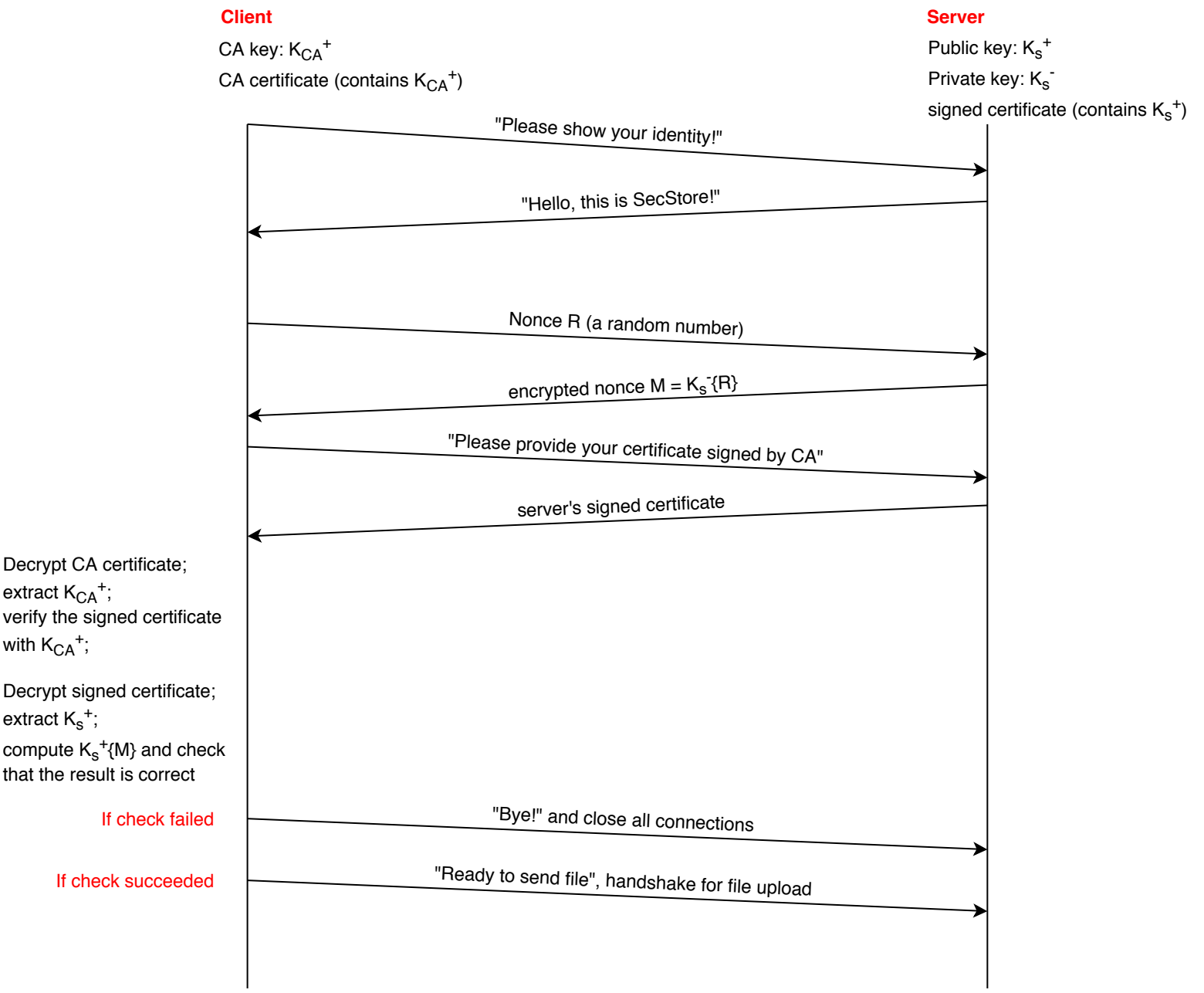
Client
CA key: K_{CA}^{+}
CA certificate (contains K_{CA}^{+})
Server
Public key: K_s^{+}
Private key: K_s^{-}
signed certificate (contains K_s^{+})
"Please show your identity!"
"Hello, this is SecStore!"
Nonce R (a random number)
encrypted nonce M = K_s^{-}{R}
"Please provide your certificate signed by CA"
server's signed certificate
Decrypt CA certificate;
extract K_{CA}^{+};
verify the signed certificate
with K_{CA}^{+};
Decrypt signed certificate;
extract K_s^{+};
compute K_s^{+}{M} and check
that the result is correct
If check failed
"Bye!" and close all connections
If check succeeded
"Ready to send file", handshake for file upload