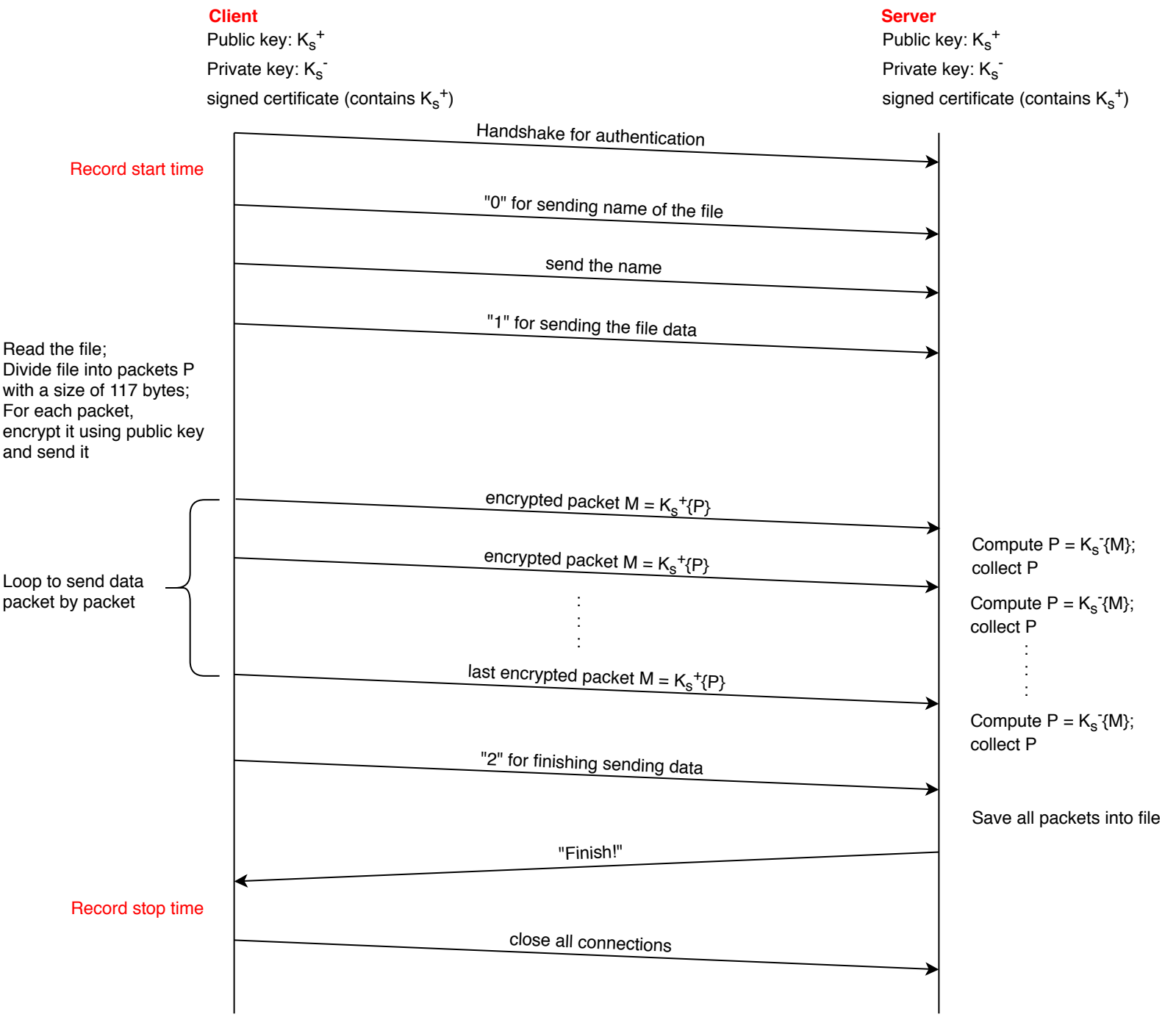
Client
Public key: K_s^+
Private key: K_s^-
signed certificate (contains K_s^+)
Server
Public key: K_s^+
Private key: K_s^-
signed certificate (contains K_s^+)
Handshake for authentication
Record start time
"0" for sending name of the file
send the name
"1" for sending the file data
Read the file;
Divide file into packets P
with a size of 117 bytes;
For each packet,
encrypt it using public key
and send it
encrypted packet M = K_s^+{P}
Loop to send data
packet by packet
encrypted packet M = K_s^+{P}
Compute P = K_s^-{M};
collect P
Compute P = K_s^-{M};
collect P
last encrypted packet M = K_s^+{P}
Compute P = K_s^-{M};
collect P
"2" for finishing sending data
Save all packets into file
"Finish!"
Record stop time
close all connections