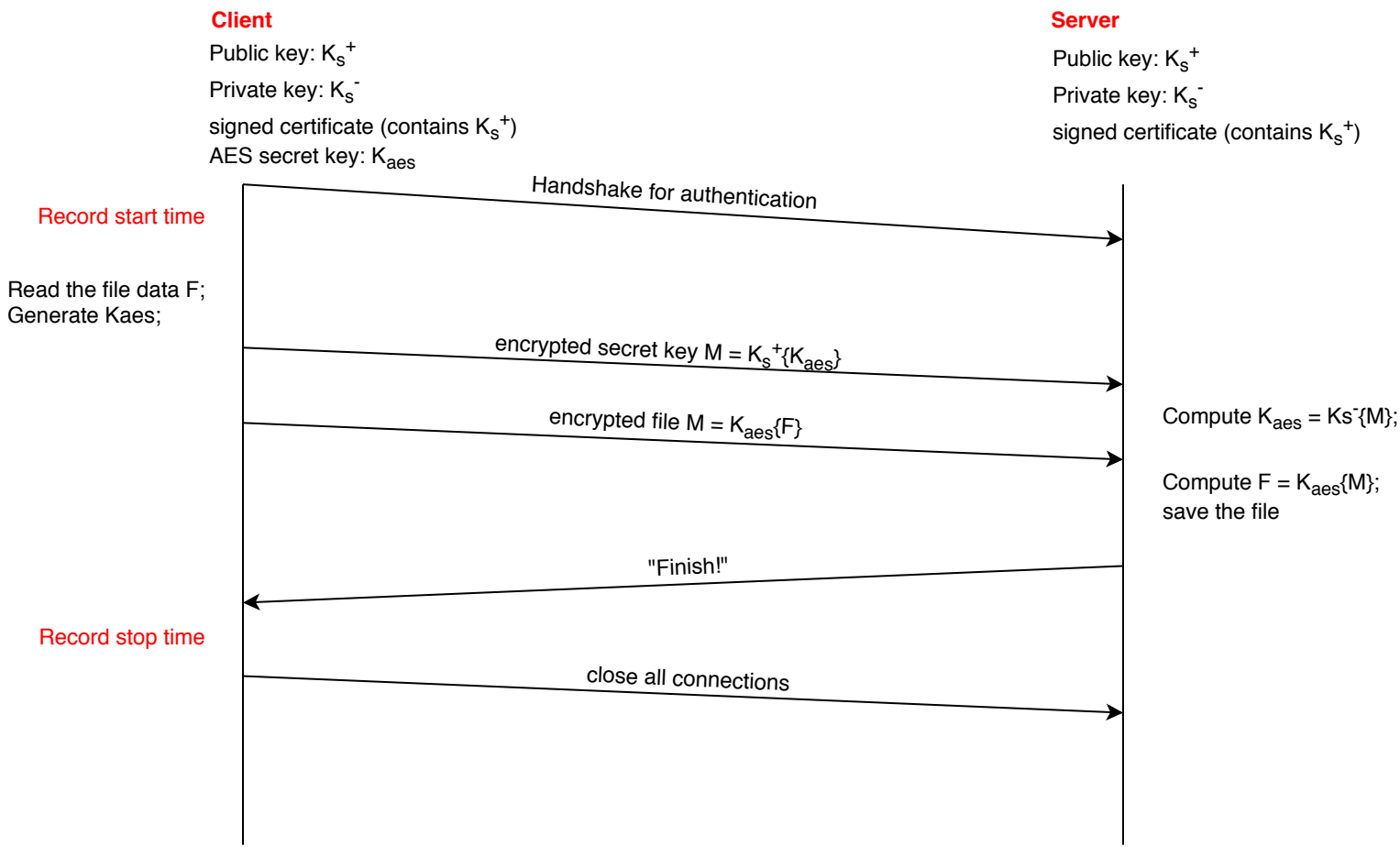
Client
Public key: K_s^+
Private key: K_s^-
signed certificate (contains K_s^+)
AES secret key: K_{aes}
Server
Public key: K_s^+
Private key: K_s^-
signed certificate (contains K_s^+)
Handshake for authentication
Record start time
Read the file data F;
Generate Kaes;
encrypted secret key M = $K_s^+\{K_{aes}\}$
encrypted file M = $K_{aes}\{F\}$
Compute K_{aes} = $Ks^-\{M\}$;
Compute F = $K_{aes}\{M\}$;
save the file
"Finish!"
Record stop time
close all connections