
























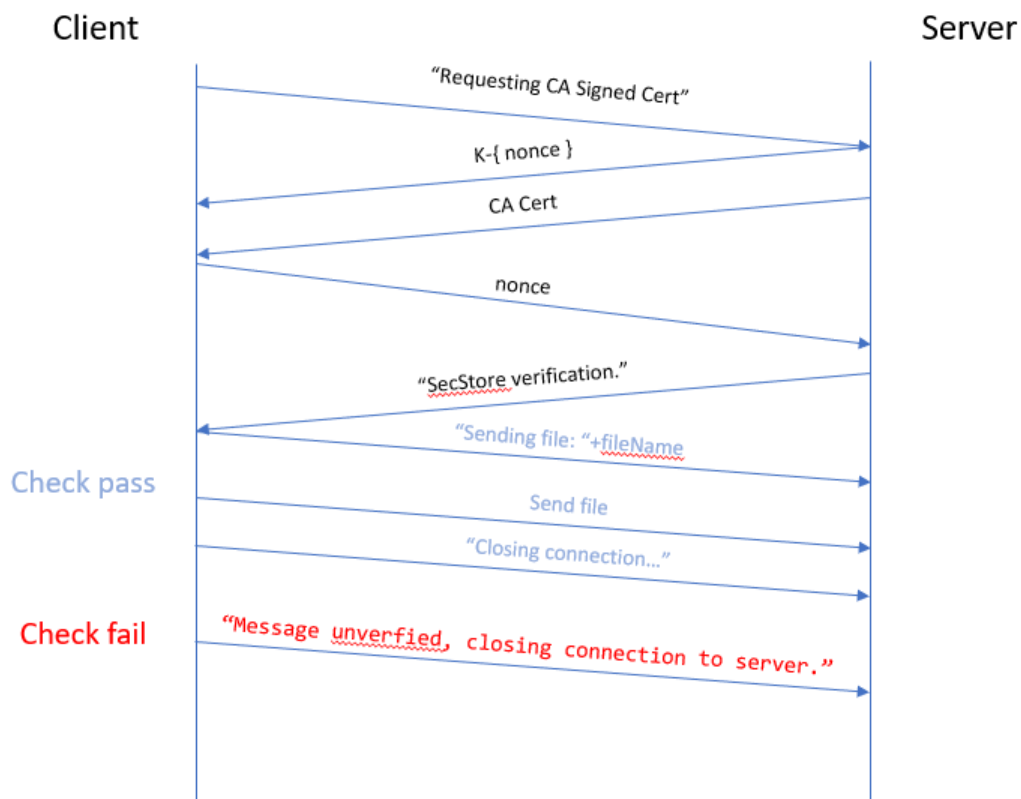
Programming Assignment 2

 Assignee	
 Created	@Jan 20, 2021 11:10 PM
 Created By	 Oei Kai Xun
 Done	<input type="checkbox"/>
 Due	@Apr 21, 2021 11:59 PM
 Edited	@Apr 21, 2021 11:53 PM
 Inbox	
 Kanban - State	To Do
 Kanban - Tag	
 Next Due	
 Parent Task	
 Priority	 Medium
 Project	 <u>50.005 Computer Systems Engineering 2021</u>
 Recur Interval (Days)	
 Start	
 State	<input type="checkbox"/>
 Sub-Tasks	
 Type	 One-Time

Specification

CP1

CP2



Problem

Problem

The client cannot tell if the public key belongs to the server or not.

Solution

By using a CA signed public key, we can verify that the public key indeed belongs to the server. This is similar to Solution 2 in case 5 of the handout.

Plots

