Programming Assignment 2
Authors: Tan Ting Yu (1002169) and Chong Lok Swen (1002468)
Date: 17/4/2018

CP-1

Firstly, the server's certificate, which is signed by the Certification Authority (CA) using the CA's private key, is sent to the client on request. The client, upon receiving the server's certificate, verifies it using the CA's public key. Secondly, the uploaded file is not encrypted, as such can be easily intercepted and interpreted. Thus, after verifying SecStore's certificate, the client should use SecStore's RSA public key to encrypt the file before sending it to SecStore. As only the SecStore knows the private key, intermediary routers and communication links will not be able to decrypt the data.

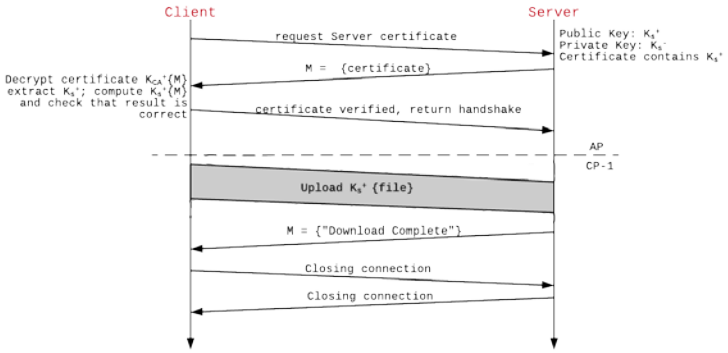

Figure 1: AP and CP-1 Specification.

CP-2

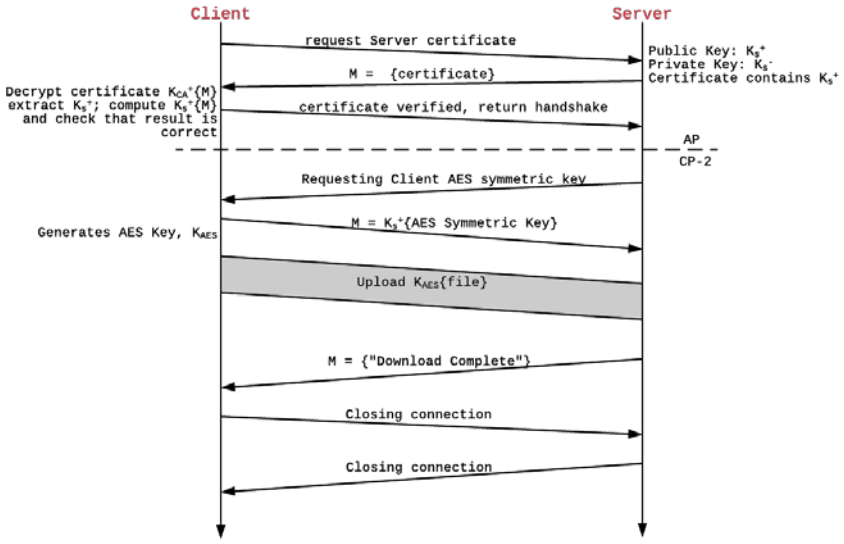

Figure 2: AP and CP-2 Specification.

File Name	File Size (bytes)	Upload Time (ms)	
		CP-1	CP-2
rr	2047652	7486.115	1641.243
ulysses	1566847	4498.788	1431.908
dataforfit	255465	850.3077	691.2032
vocab	20240	530.7098	508.9372
onedaydiffs	6837	478.3206	470.6343

Table 1: Upload time of files with different sizes.

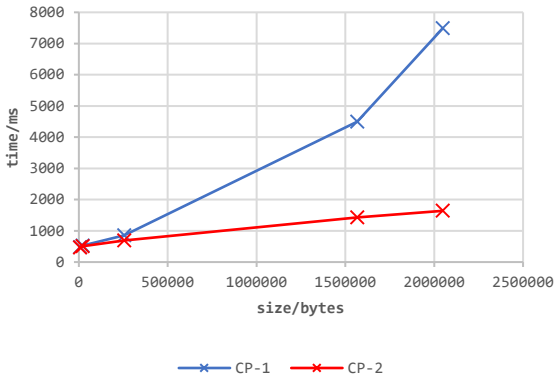

Figure 3: Graph of upload time against file size.

For small file sizes, the performance of both CP-1 and CP-2 are similar. However, from the above graph, CP-1's line has a much steeper gradient than that of CP-2, the time taken by CP-1 increasing significantly quicker than CP-2 as the file sizes become larger. Hence, CP-2 is the more practical choice.