CMPE 272 – HW#7

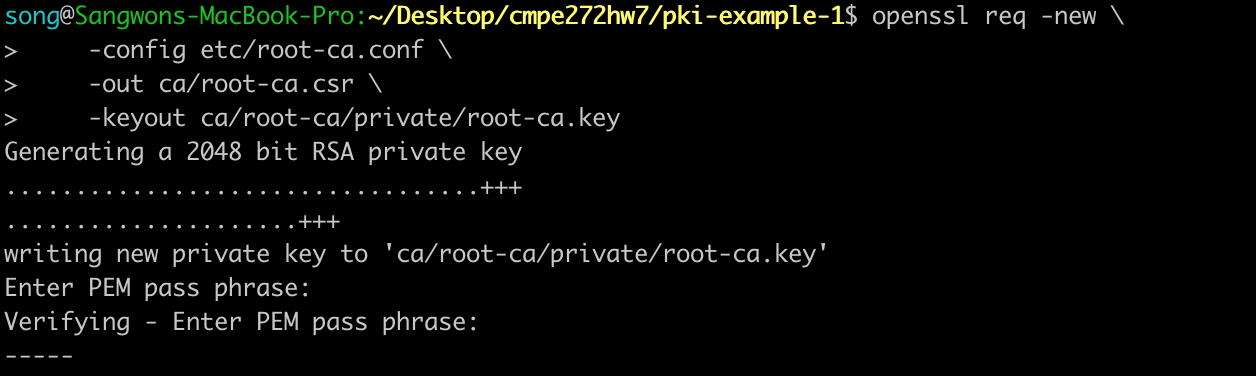
Crack It – Sangwon Song, Yunting Xiang, Junteng Ton

**Security**

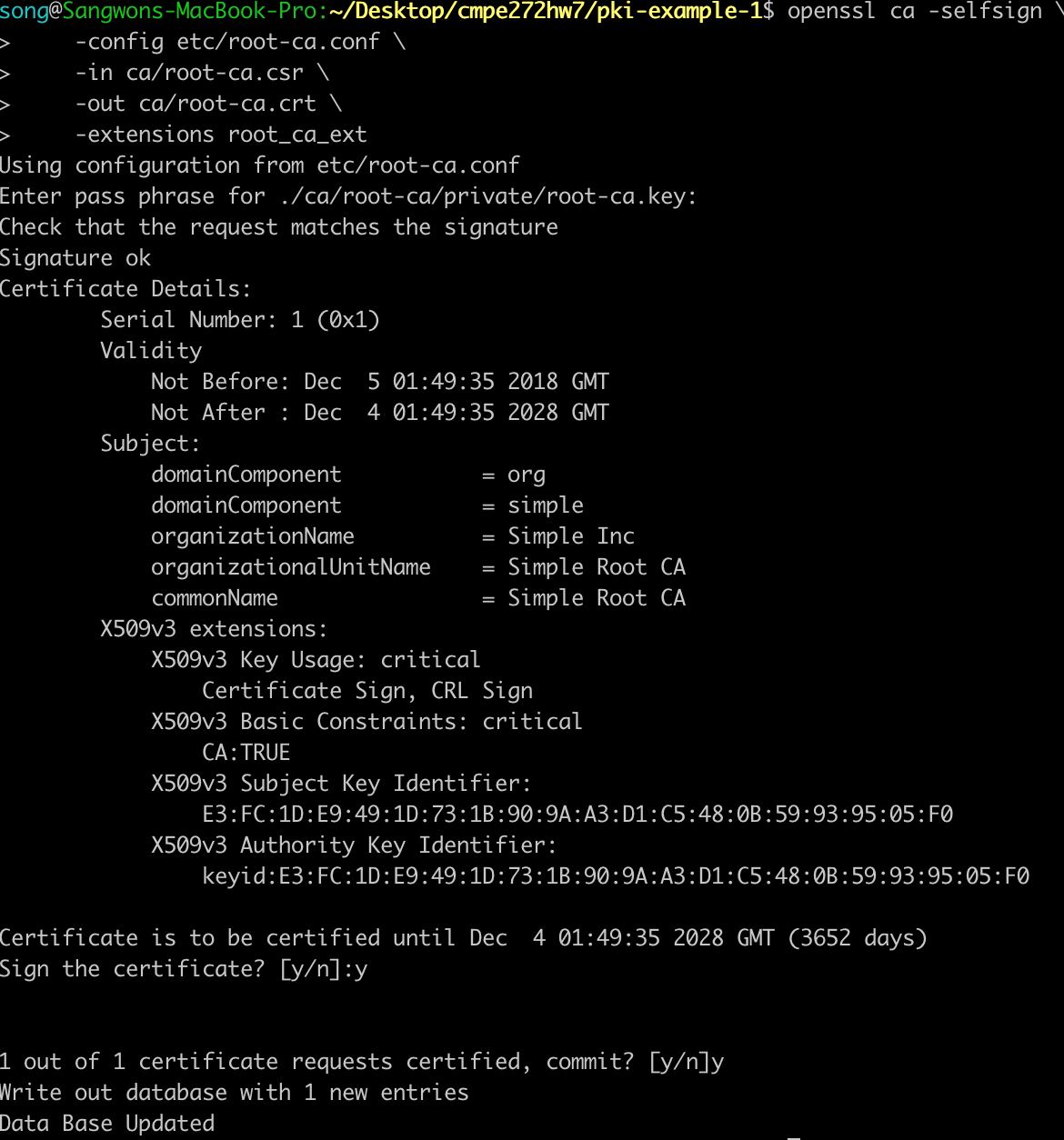
**Part 1. Design and build a PKI infrastructure including Root CA, Signing CA, TLS Certificate**

The step-by-step is described at https://pki-tutorial.readthedocs.io/en/latest/simple/

1. Create CA request for Root CA



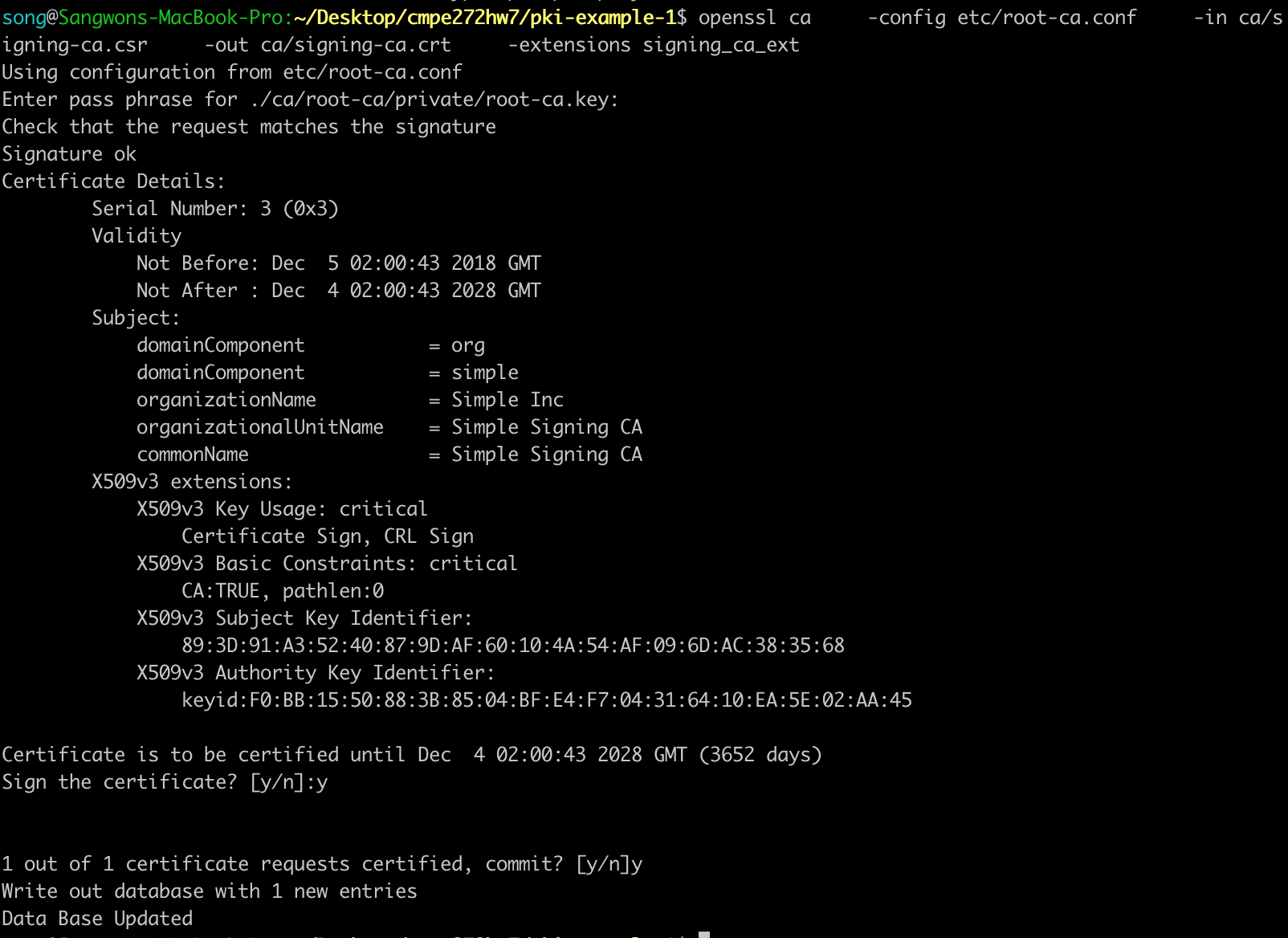
2. Create CA certificate for Root CA



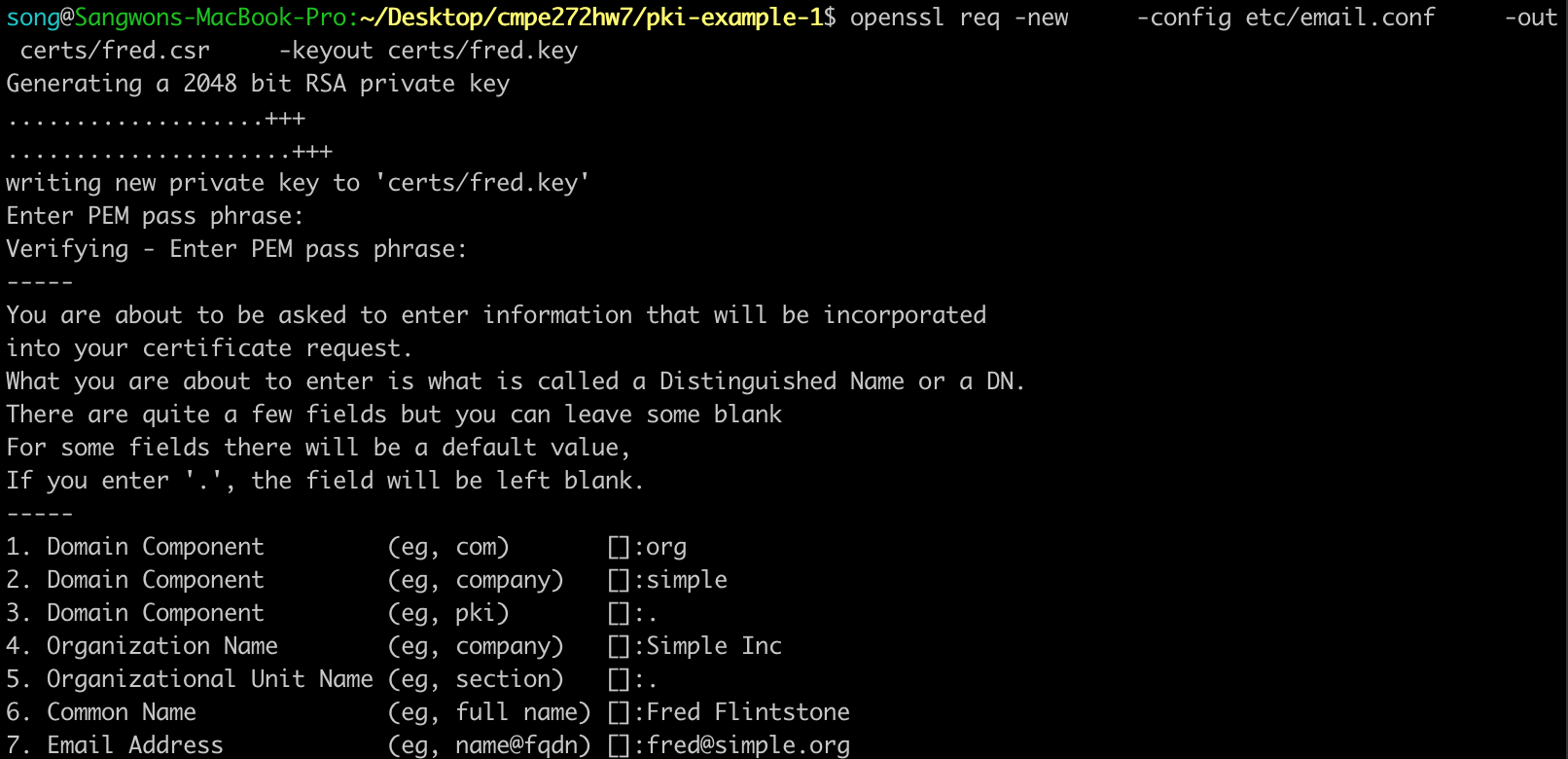
3. Create CA request for Signing CA



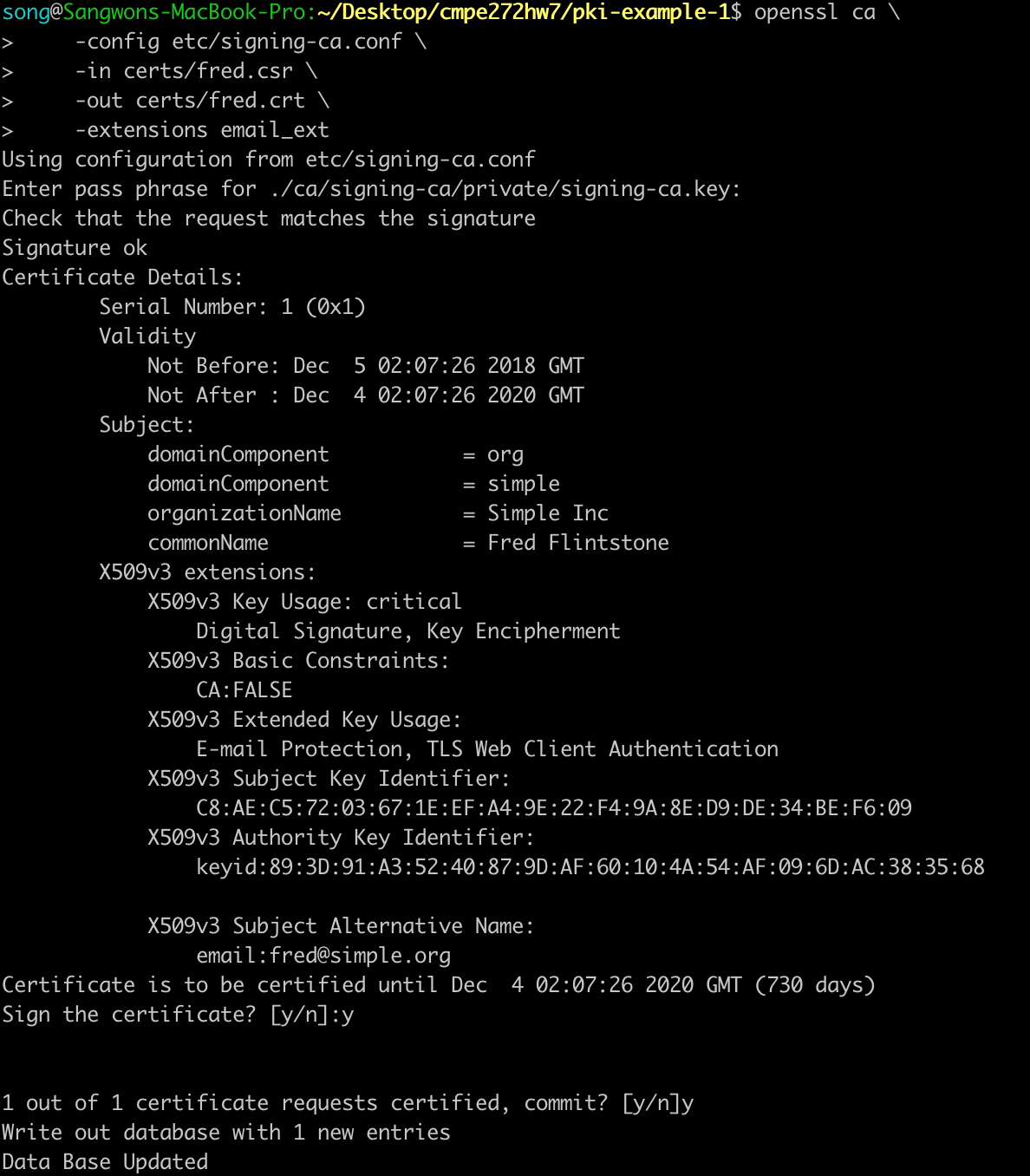
4. Create CA certificate for Signing CA



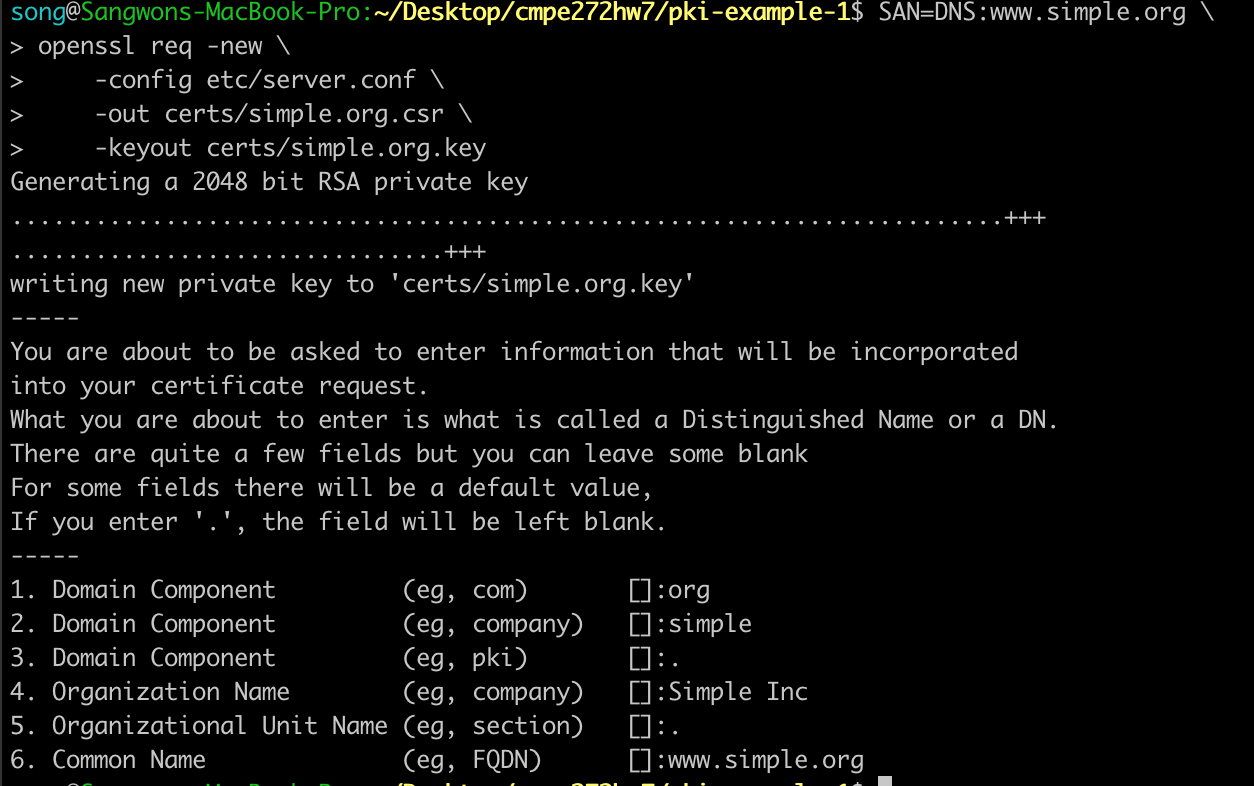
5. Create email request



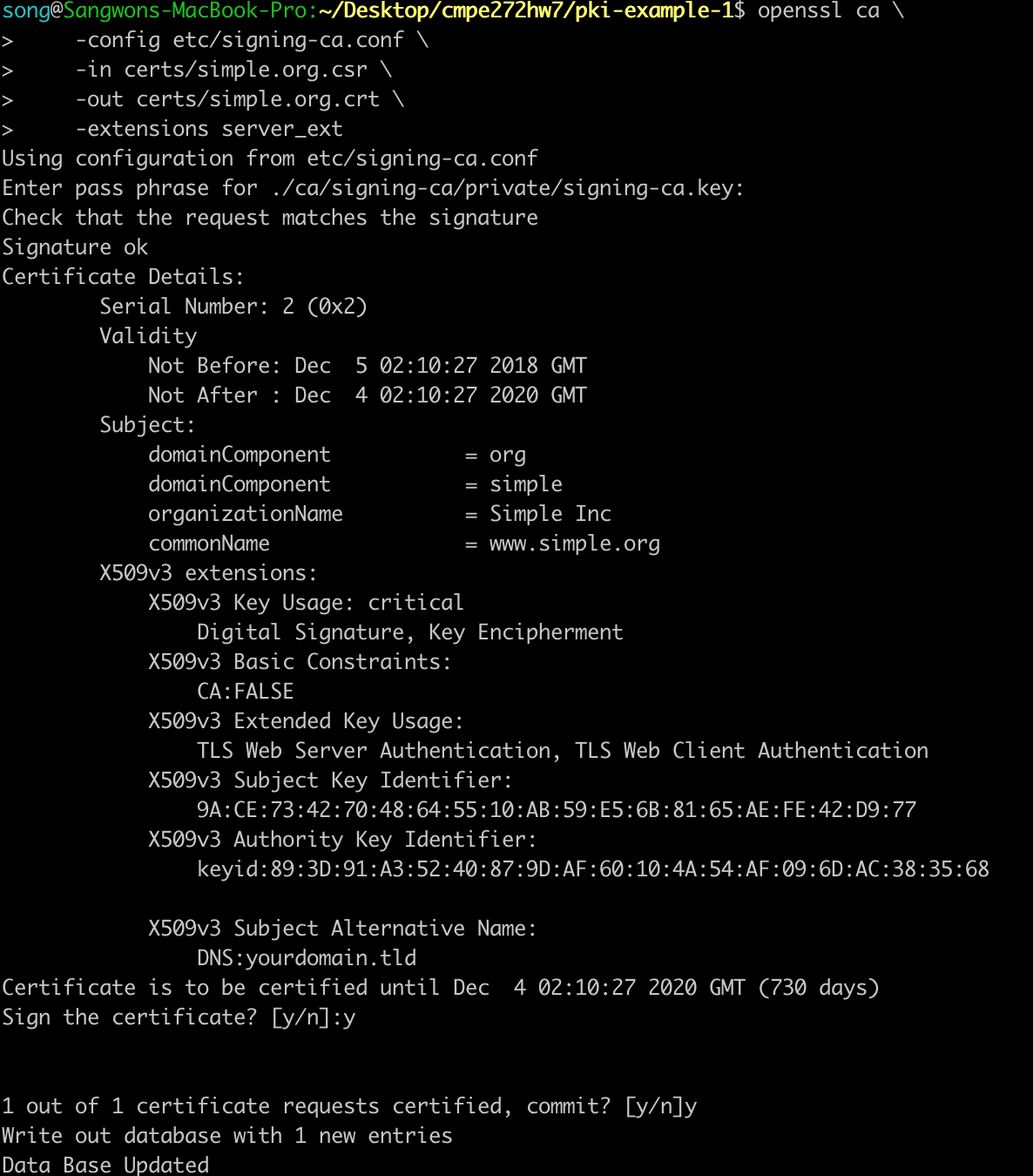
6. Create email certificate



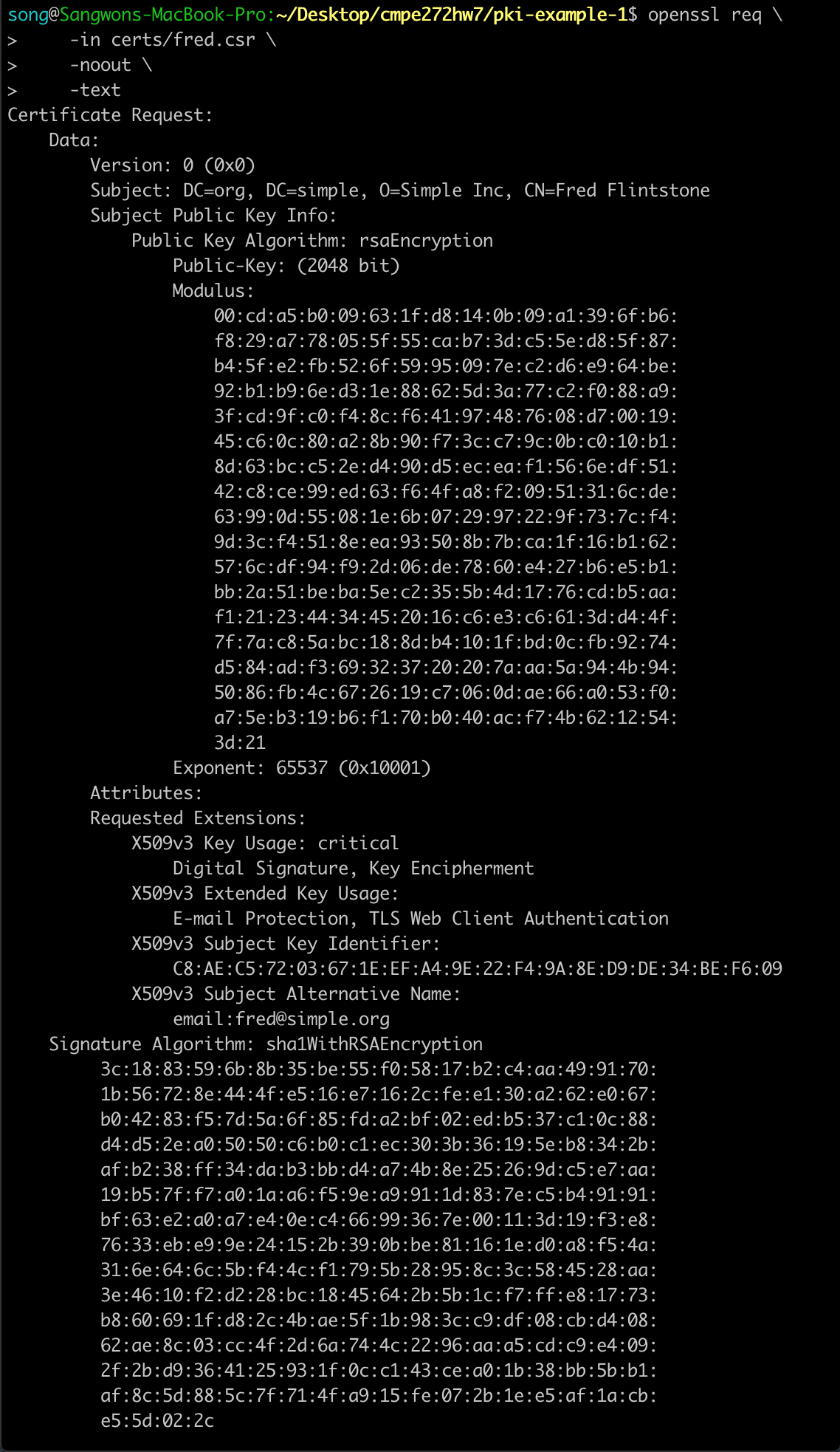
7. Create TLS server request



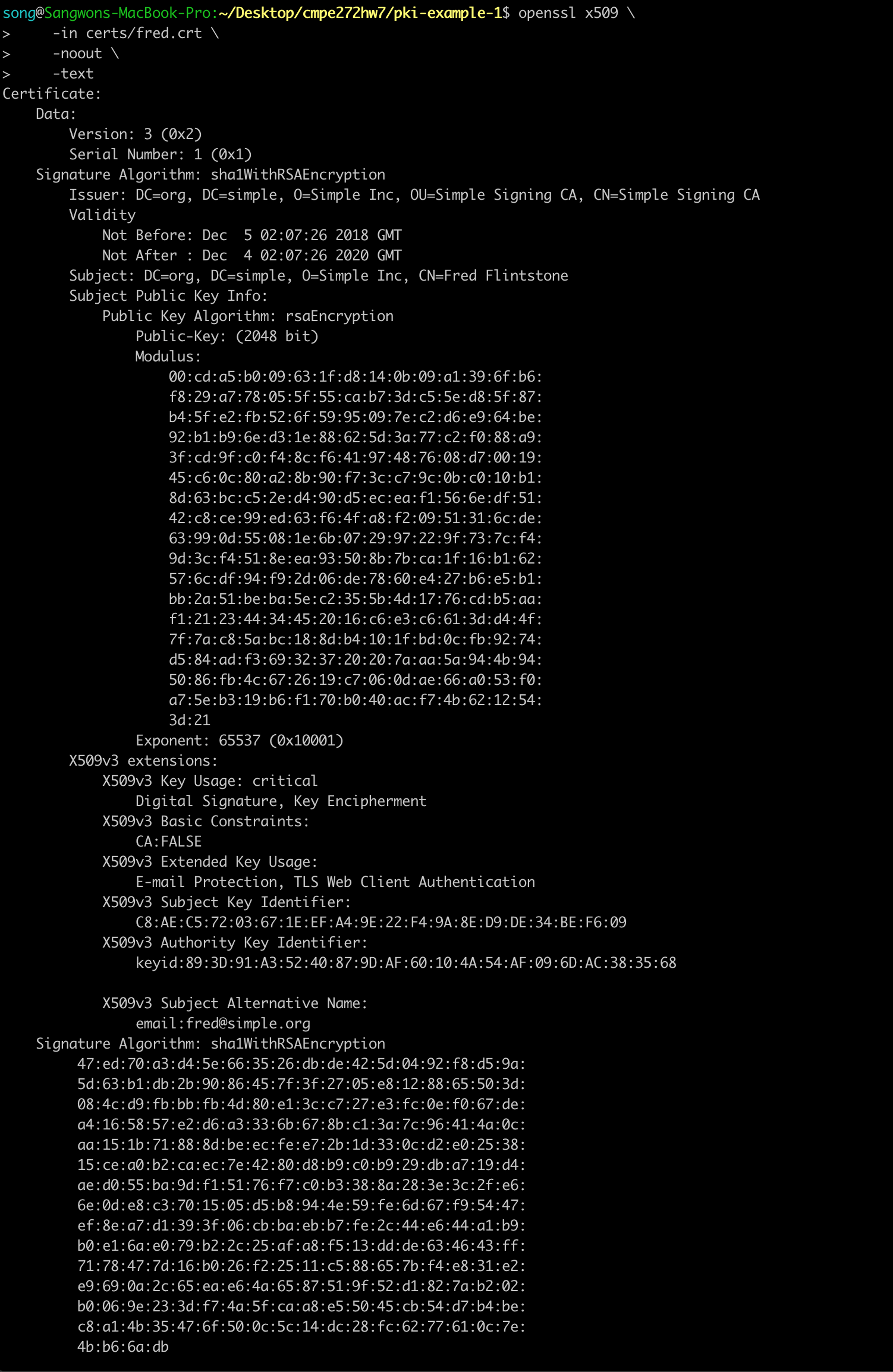
8. Create TLS server certificate



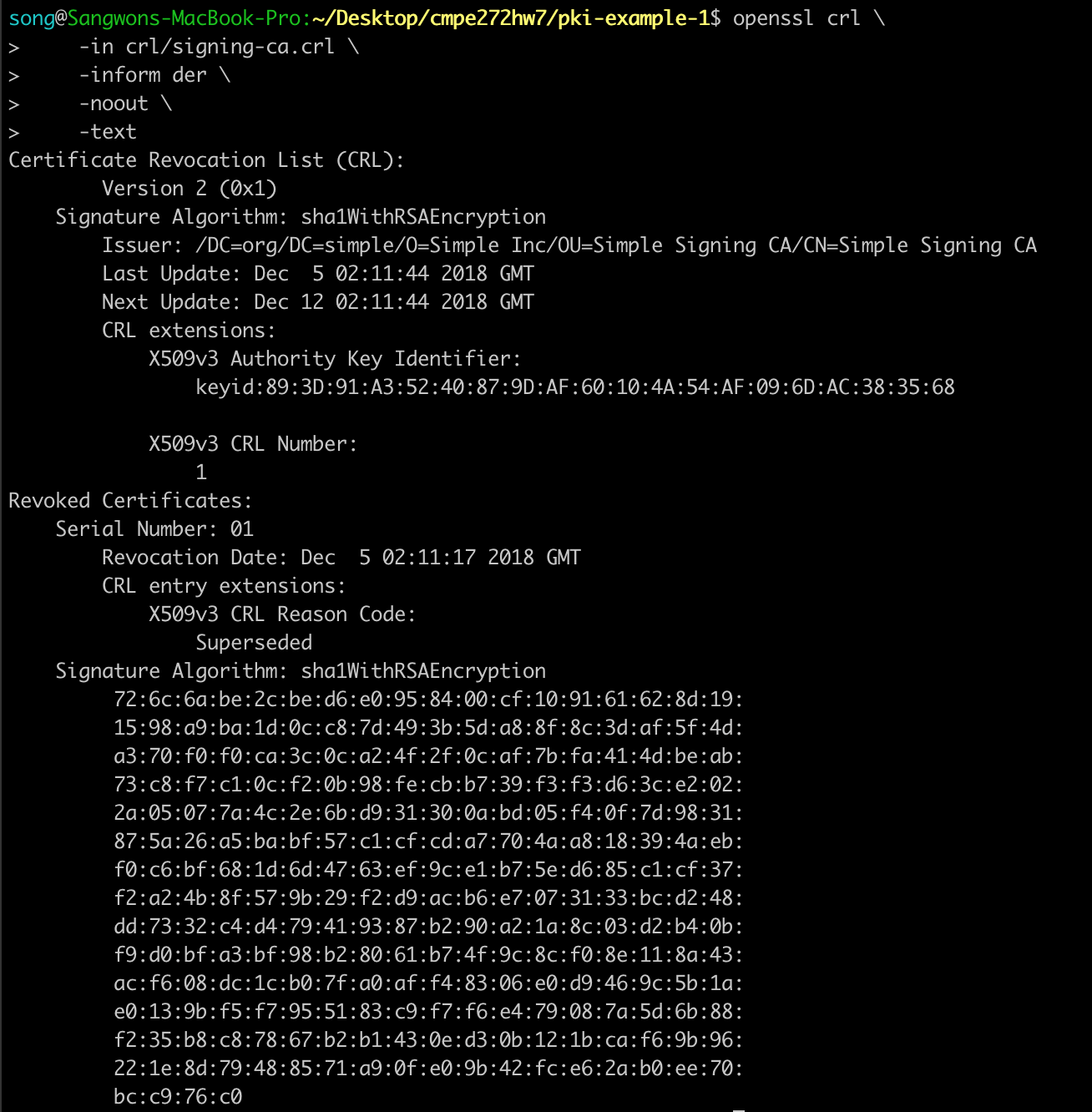
9. View Request



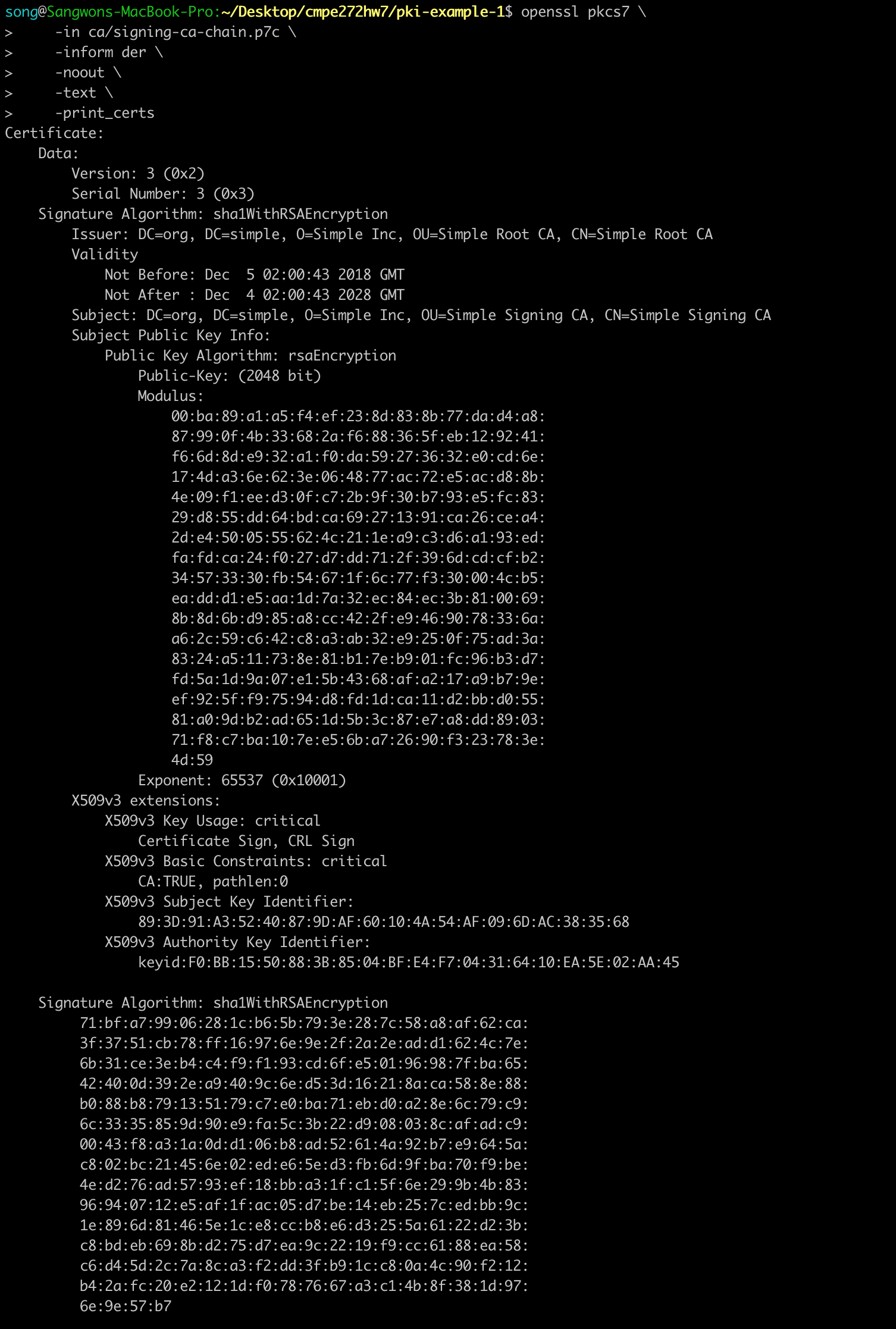
10. View Certificate



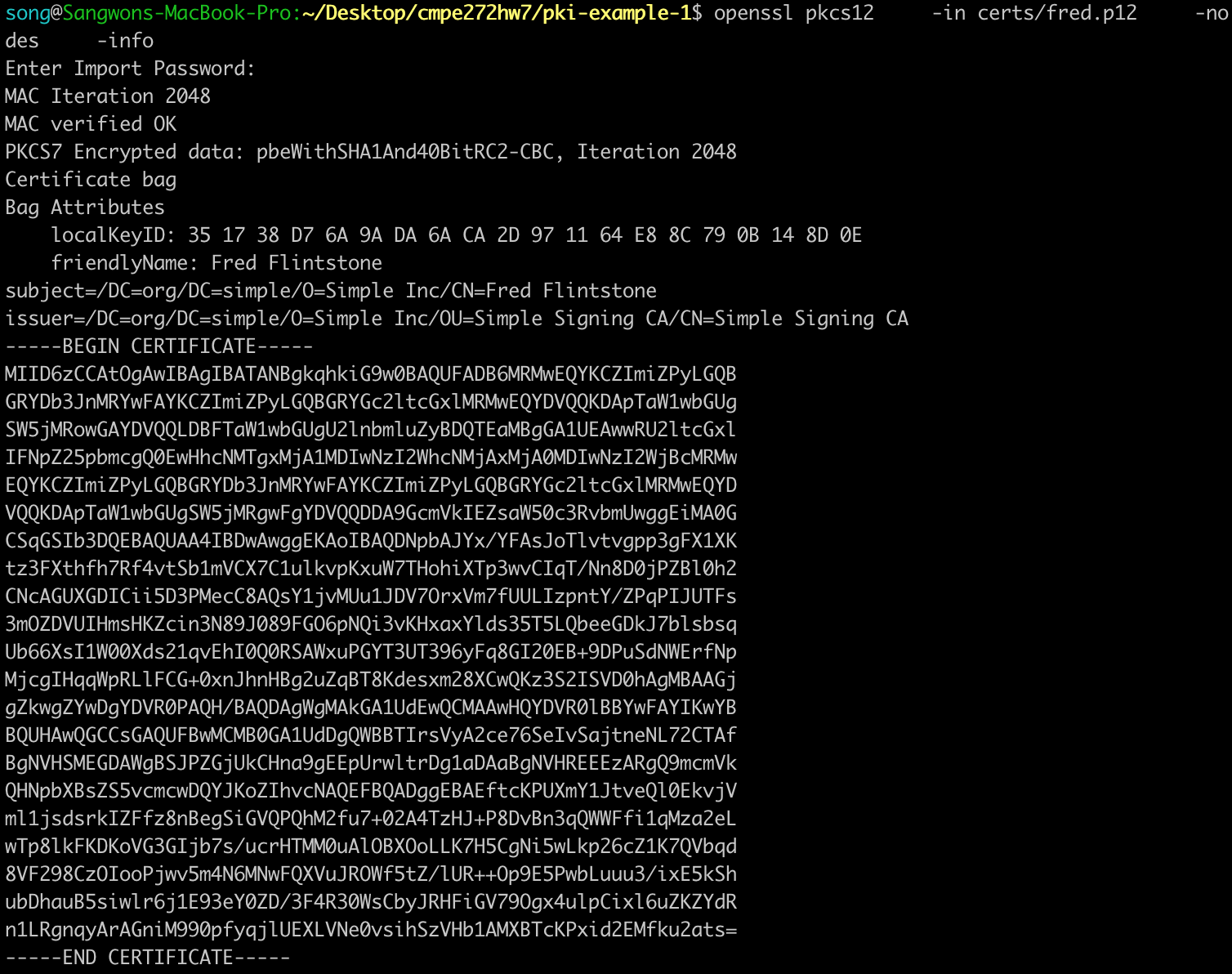
11. View CRL



12. View PKCS#7 Bundle





13. View PKCS#12 Bundle

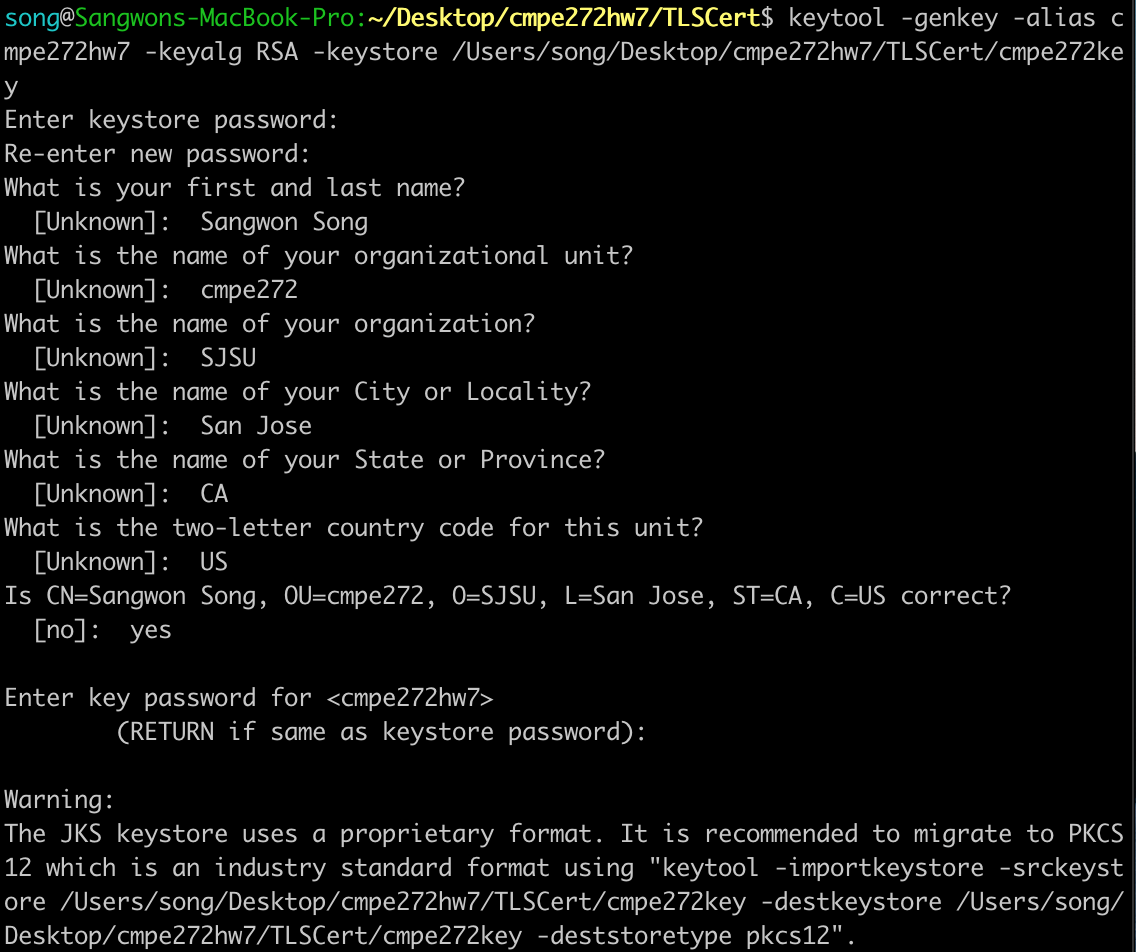


**Part 2. Use the TLS/SSL Certificate to install a web server**

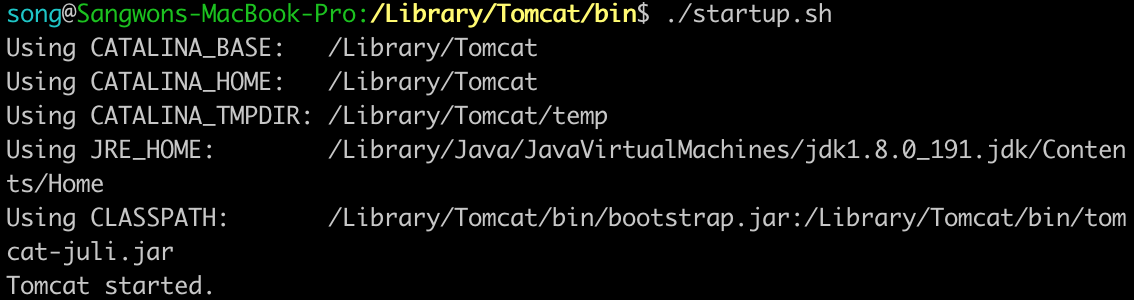
For this part, we used the public SSL certificate.

1. Environment Setup

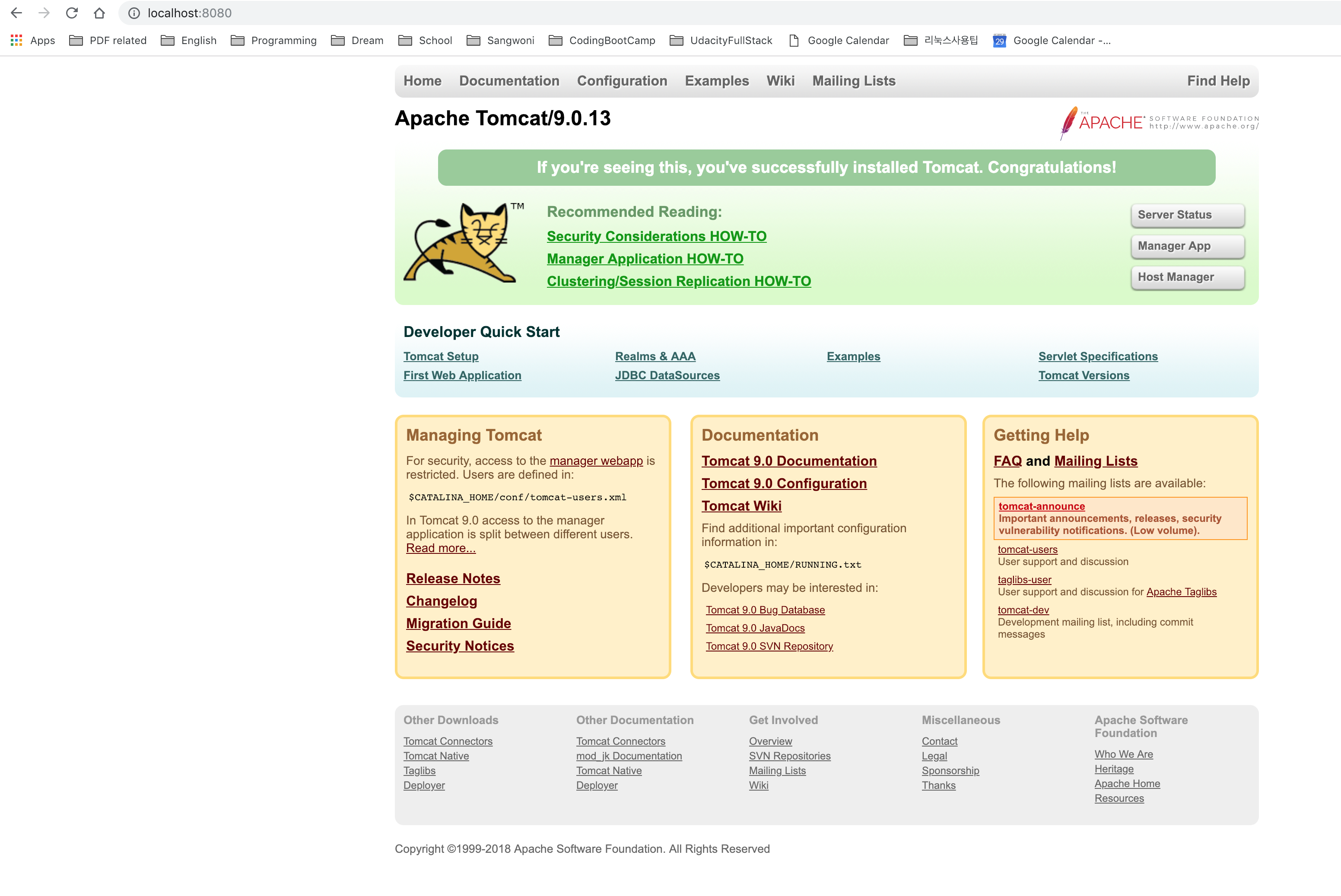
1.1 Generate a Secure Key



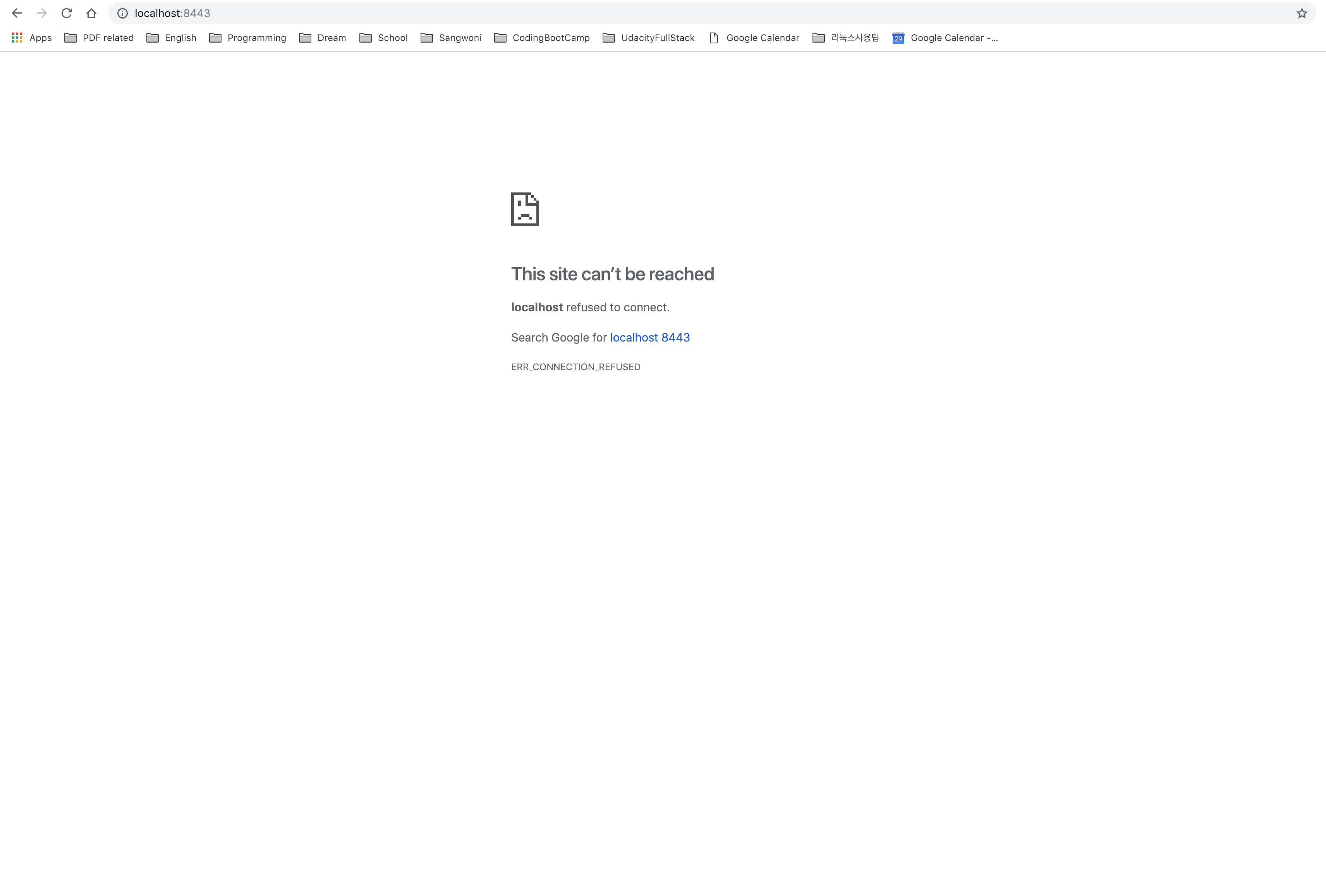
1.2 Install Tomcat Server and Start the Server



We can check if it is running on localhost:8080

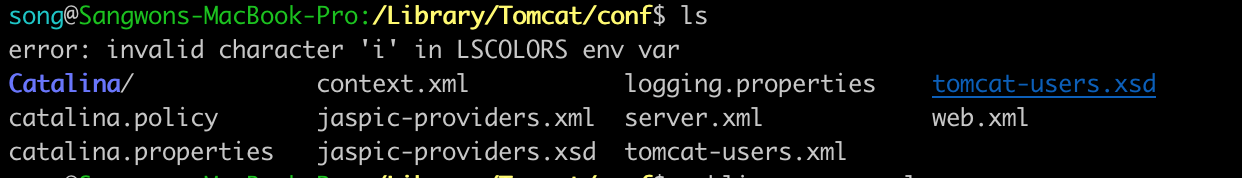


On the port 8443, the website cannot be accessible, and we will make it enabled with SSL certificate.

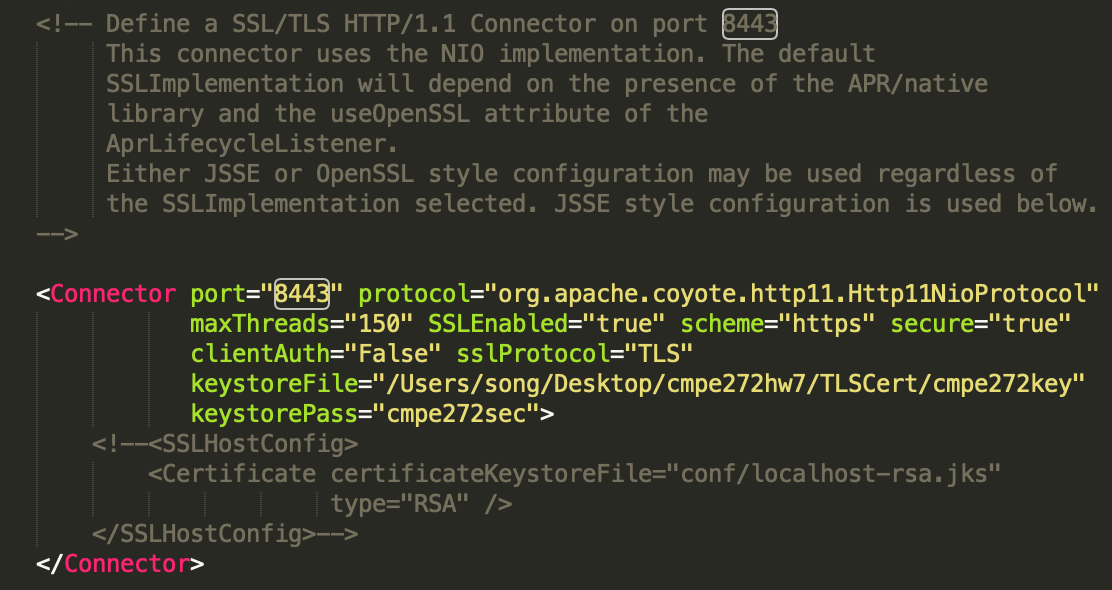


2. Create Certificate

2.1 Navigate to the Tomcat Configuration file and Modify server.xml

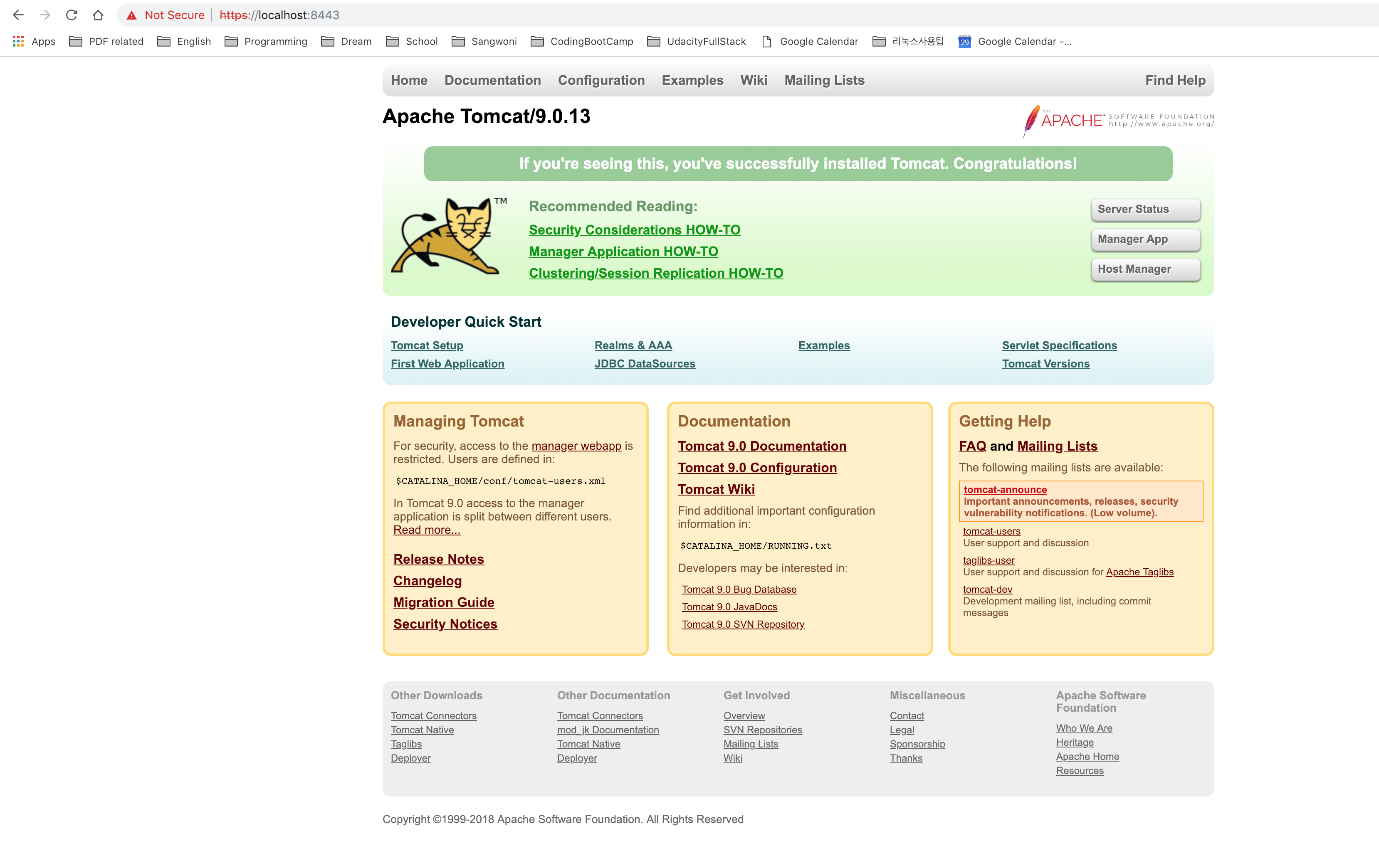


Modify with the certificate key and its password



3. Check the Connection

Restart the Tomcat server and check if Port 8443 can be accessible with the certificate.



**Github repository: https://github.com/ssong86/cmpe272-hw7-fall2018**