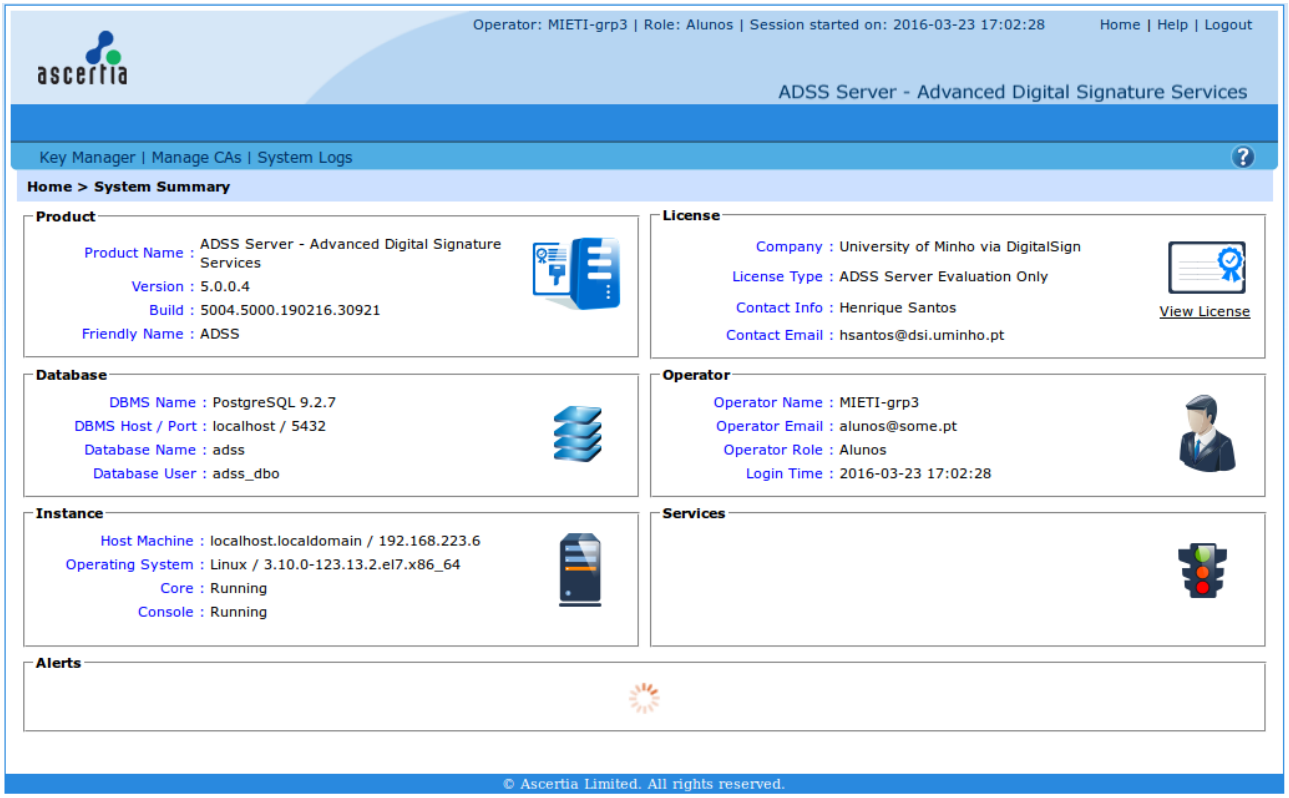
UC: Segurança de Redes e Computadores

TP3 – Certificates and PKIs

Work Logbook by Group 3

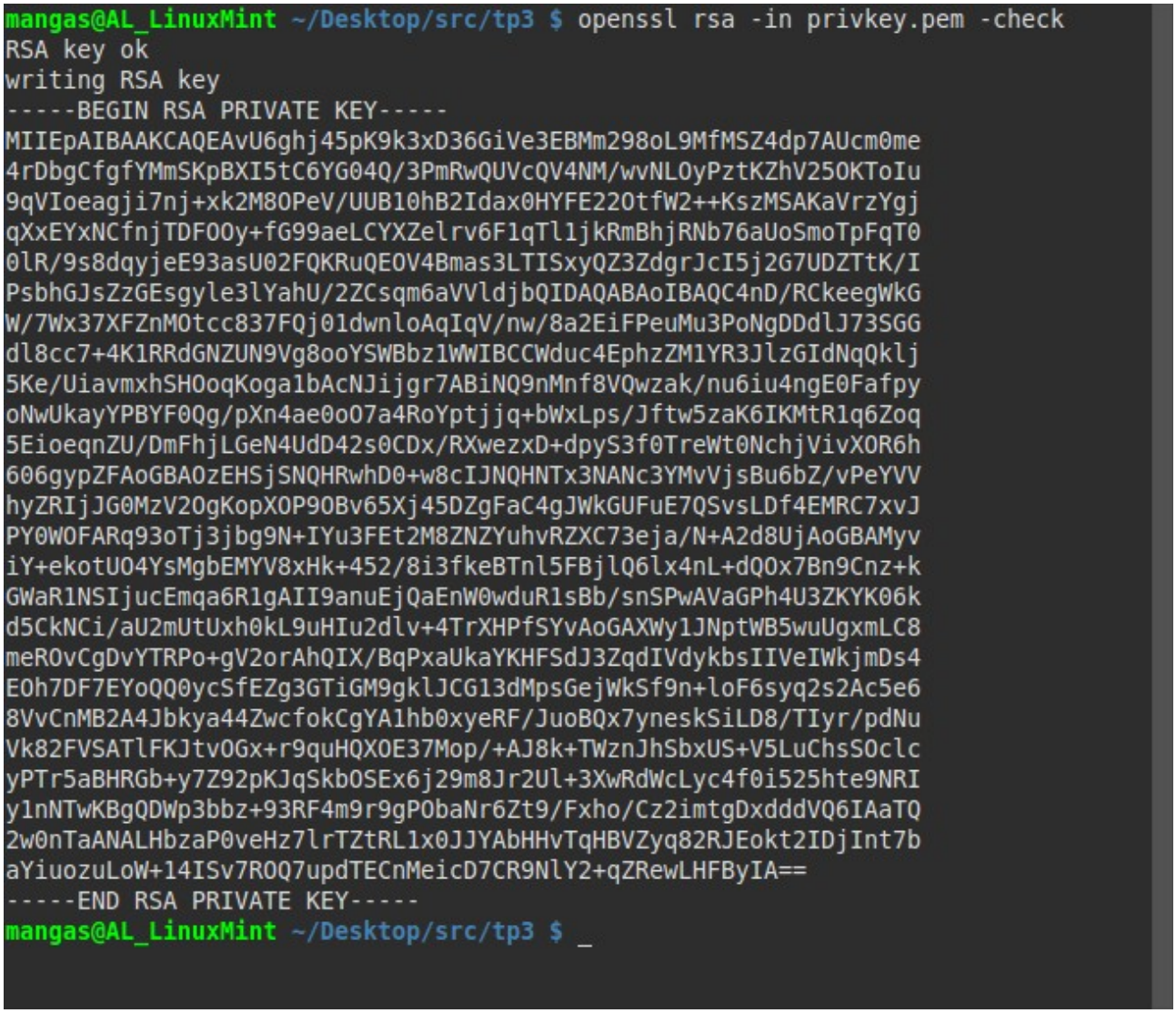
This logbook will be divided in a way that matches the given exercises.

1. First of all we gained access to the adss server through a vpn and after installing several needed components. Here we can see it's home page.



2. Since we am working in a Linux environment, specifically Linux Mint 17.2, OpenSSL already comes installed in the base packages.

3. In this step we had to create a pair of keys, one private and the other public. This was done with the command *openssl genrsa -out privkey.pem 2048*. The following image shows a state check of the key.



4. Next we had to create a certificate request, again using OpenSSL. In the image we can see the created request.

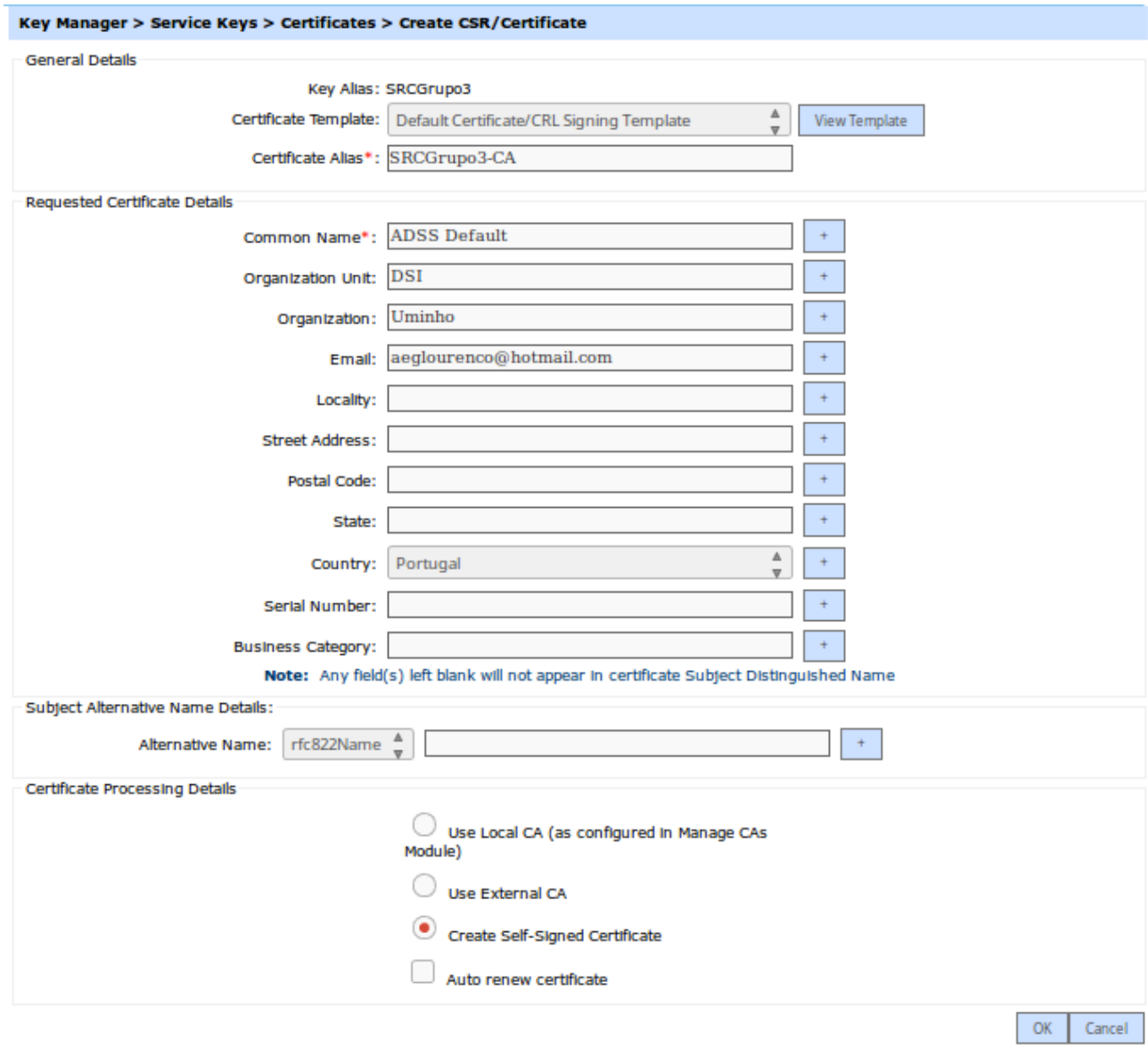
```
mangas@AL_LinuxMint ~/Desktop/src/tp3 $ openssl req -text -noout -verify -in cert.csr
verify OK
Certificate Request:
    Data:
        Version: 0 (0x0)
        Subject: C=PT, ST=Braga, L=Guimaraes, O=Universidade do Minho, CN=Antonio/emailAddress=aeglourenco@hotmail.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:bd:4e:a0:86:3e:39:a4:af:64:df:10:f7:e8:68:
                    95:7b:71:01:32:6d:bd:f2:82:fd:31:f3:12:67:87:
                    69:ec:05:1c:9b:49:9e:e2:b0:db:80:27:e0:7d:83:
                    26:48:aa:41:5c:8e:6d:0b:a6:06:d3:84:3f:dc:f9:
                    91:c1:05:15:71:05:78:34:cf:f0:bc:d2:ce:c8:fc:
                    ed:29:98:55:db:93:8a:4e:82:2e:f6:a5:48:a1:e6:
                    a0:8e:2e:e7:8f:ec:64:d8:cf:0e:3d:e5:7f:51:40:
                    75:d2:10:76:21:d6:b1:d0:76:05:13:6d:8e:b5:f5:
                    b6:fb:e2:ac:cc:c4:80:29:a5:6b:cd:88:23:a9:7c:
                    44:63:13:42:7e:78:d3:0c:53:8e:cb:e7:c6:f7:d6:
                    9e:2c:26:17:65:e9:6b:bf:a1:75:a9:39:75:8e:44:
                    66:06:18:d1:35:be:fa:69:4a:12:9a:84:e9:16:a4:
                    f4:d2:54:7f:f6:cf:1d:ab:28:de:13:dd:da:b1:4d:
                    36:15:02:91:b9:01:0e:57:80:66:6a:cd:cb:4c:84:
                    b1:c9:06:77:65:d8:2b:25:c2:39:8f:61:bb:50:36:
                    53:b4:af:c8:3e:c6:e1:18:9b:19:cc:61:2c:83:29:
                    5e:de:56:1a:85:4f:f6:64:2b:2a:9b:a6:95:56:57:
                    63:6d
                Exponent: 65537 (0x10001)
        Attributes:
            unstructuredName         :unable to print attribute
    Signature Algorithm: sha256WithRSAEncryption
         b8:09:24:87:65:a8:43:73:ee:a0:cf:d5:ba:70:36:00:c5:c1:
         fe:01:fd:21:c2:e1:0a:a3:e3:01:00:58:ee:ae:dd:9f:06:f4:
         19:ba:73:43:7c:fd:ec:01:96:ae:d3:16:91:33:38:d6:d2:1f:
         cc:90:d4:c4:41:04:93:20:de:3c:c7:d6:46:56:52:7c:0a:ce:
         c6:aa:1b:22:e8:5c:48:43:7a:33:c4:1a:c3:f9:7a:97:ed:a7:
         56:92:1d:84:58:09:3e:14:77:5f:7c:ff:fc:9e:da:f4:30:fc:
         d3:ae:1d:16:ee:18:f6:f0:04:6f:39:74:39:92:45:6e:45:75:
         99:d3:04:1f:0b:2d:03:1a:1b:8c:31:63:da:75:1e:96:72:3d:
         40:20:2f:4f:e5:83:c4:3f:8c:79:f6:a3:df:45:49:90:f2:9d:
         87:05:00:44:11:27:bf:c5:a7:76:00:0c:34:fa:77:6a:ff:42:
         3e:5d:12:da:65:00:92:a5:4c:b0:eb:c3:53:8b:de:19:88:ac:
         bd:a7:dc:e9:ef:bd:66:b8:db:d6:31:82:1d:b7:e4:b4:94:fb:
         21:52:64:d1:8d:fb:68:66:04:b4:ec:fd:c6:d5:ea:9f:f9:74:
         ef:b1:09:ff:11:0b:75:a1:6e:7f:6a:ff:25:c6:7e:15:4f:f9:
         65:ac:aa:12
```

5. The next step was to combine the private key and the certificate request into a self signed certificate.

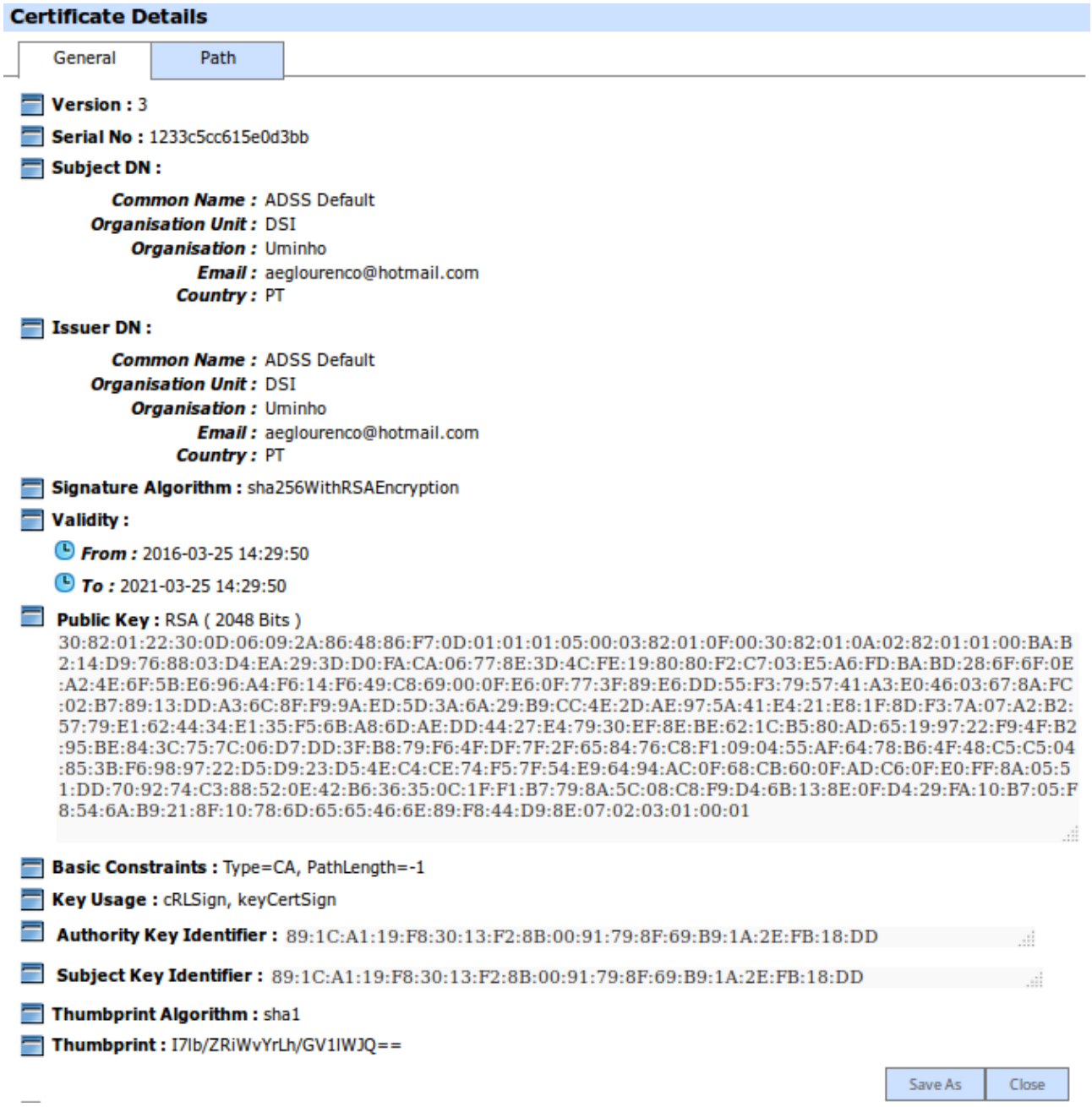
```
mangas@AL_LinuxMint ~/Desktop/src/tp3 $ openssl x509 -req -in cert.csr -signkey
privkey.pem -out privcert.crt
Signature ok
subject=/C=PT/ST=Braga/L=Guimaraes/O=Universidade do Minho/CN=Antonio/emailAddre
ss=aeglourenco@hotmail.com
Getting Private key
mangas@AL_LinuxMint ~/Desktop/src/tp3 $ _
```

6. In this step we had to access the adss server and request a public certificate.

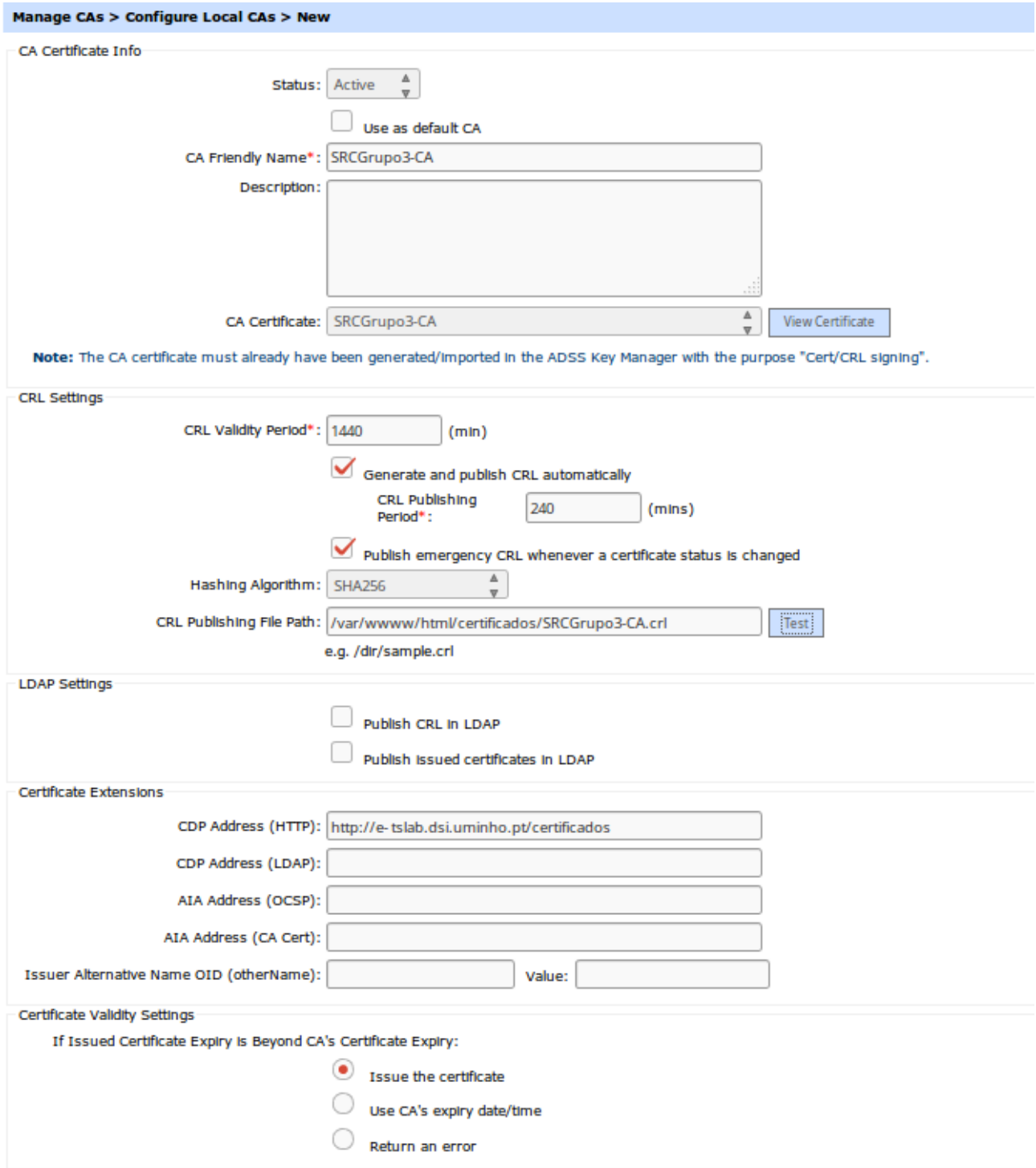
7. At this moment it was time to create a CSR/Certificate



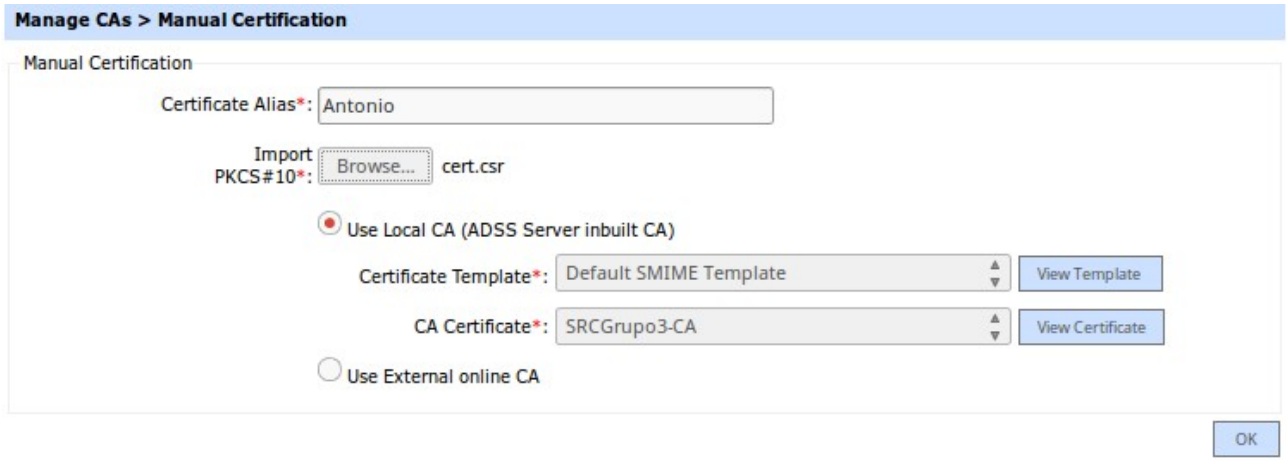
8. This step implicated only that we printed the details of the certificate we had created before.



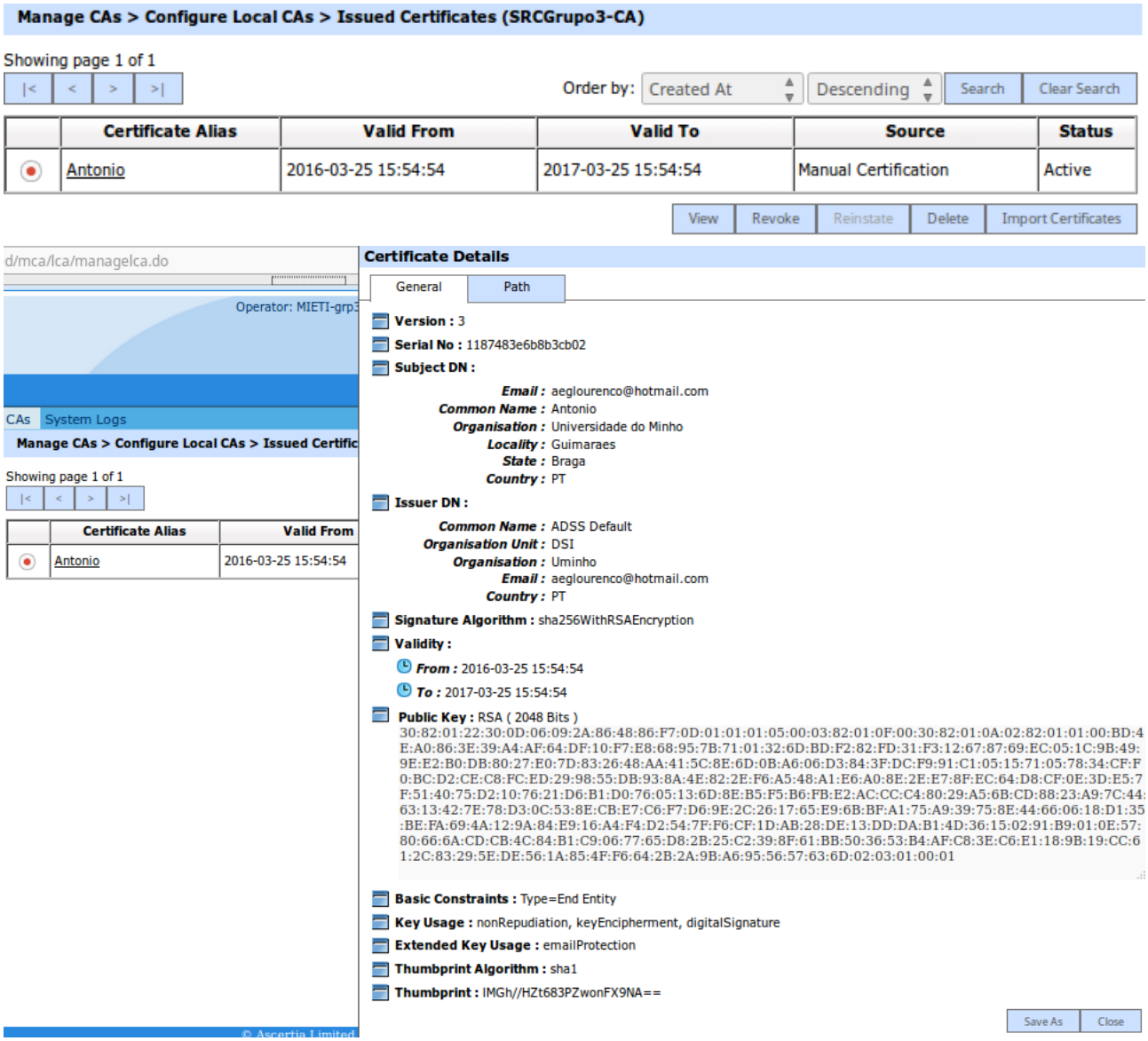
9. In this step we had to create a CA.



10. This time each one of us had to create a personal certificate.



11. Prints respectively of the issued Certificates and a personal certificate.

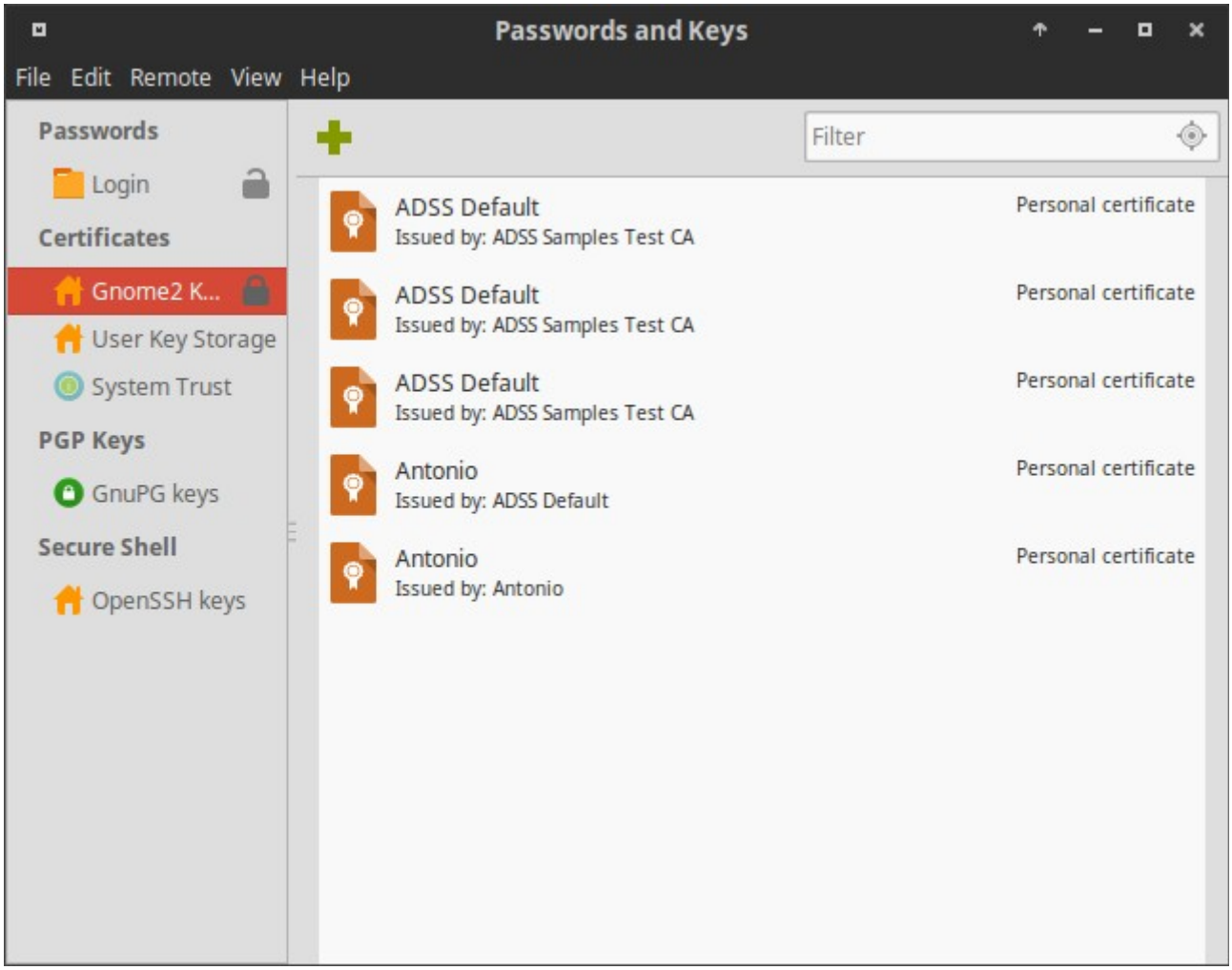


12. Now we had to combine each private key with the certificate issued for each of us. First we had to change the file extension of the certificates.

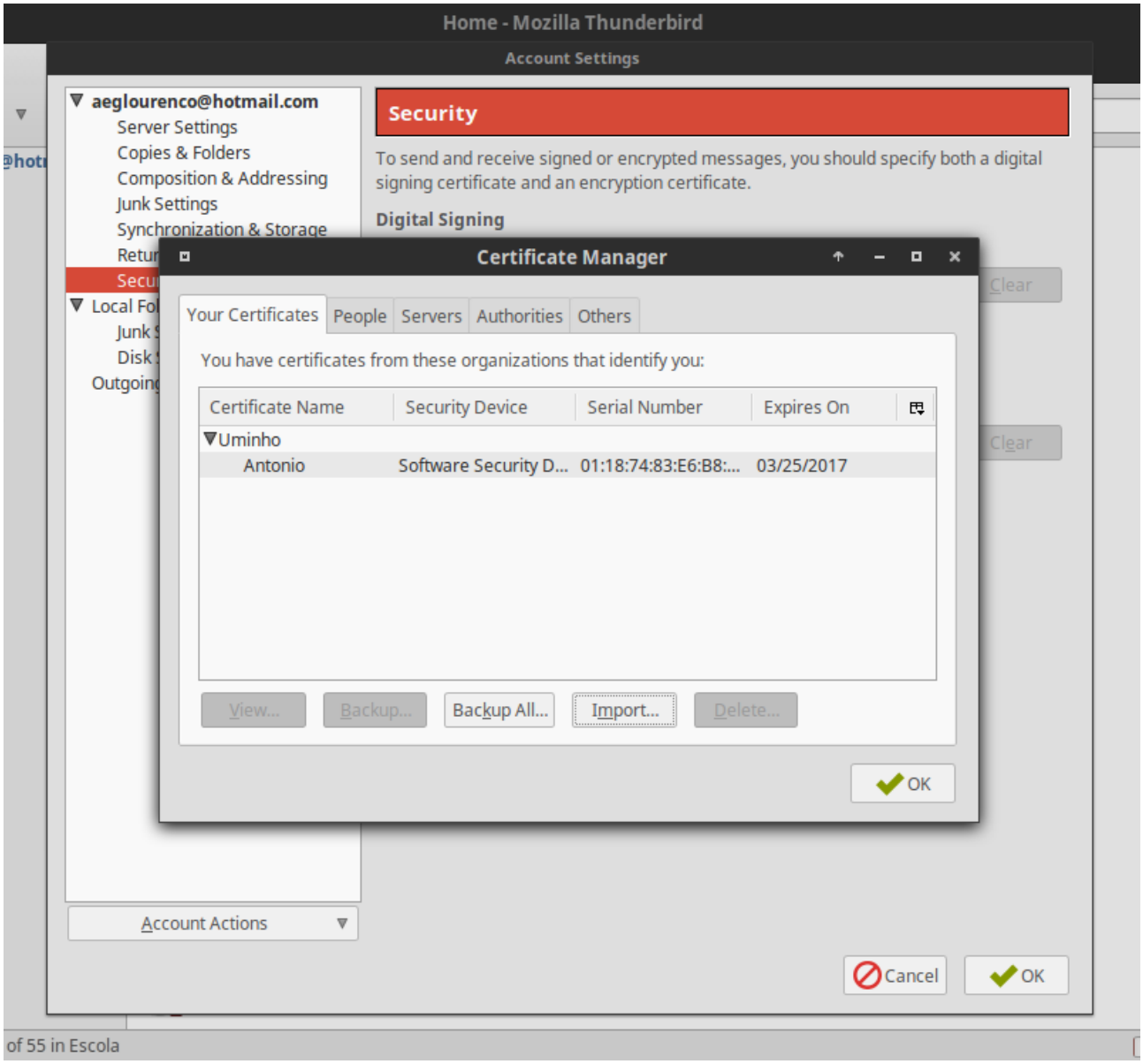
```
Terminal
mangas@AL_LinuxMint ~/Desktop/src/tp3 $ openssl x509 -inform der -in personalcer
tificate.cer -out percert.pem
mangas@AL_LinuxMint ~/Desktop/src/tp3 $ openssl x509 -inform der -in CAcert.cer
-out CAcert.pem
mangas@AL_LinuxMint ~/Desktop/src/tp3 $ _
```

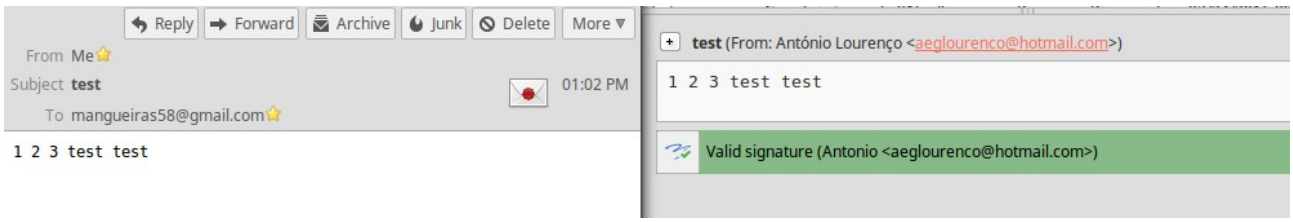
```
Terminal
mangas@AL_LinuxMint ~/Desktop/src/tp3 $ openssl pkcs12 -export -in percert.pem -inkey privkey.
pem -certfile CAcert.pem -name "Antonio" -out priv-pkcs12.p12
Enter Export Password:
Verifying - Enter Export Password:
mangas@AL_LinuxMint ~/Desktop/src/tp3 $ _
```

13. Now we had to import all of this certificates to the OS. Here we can see the program *Passwords and Keys* that manages the certificates imported.

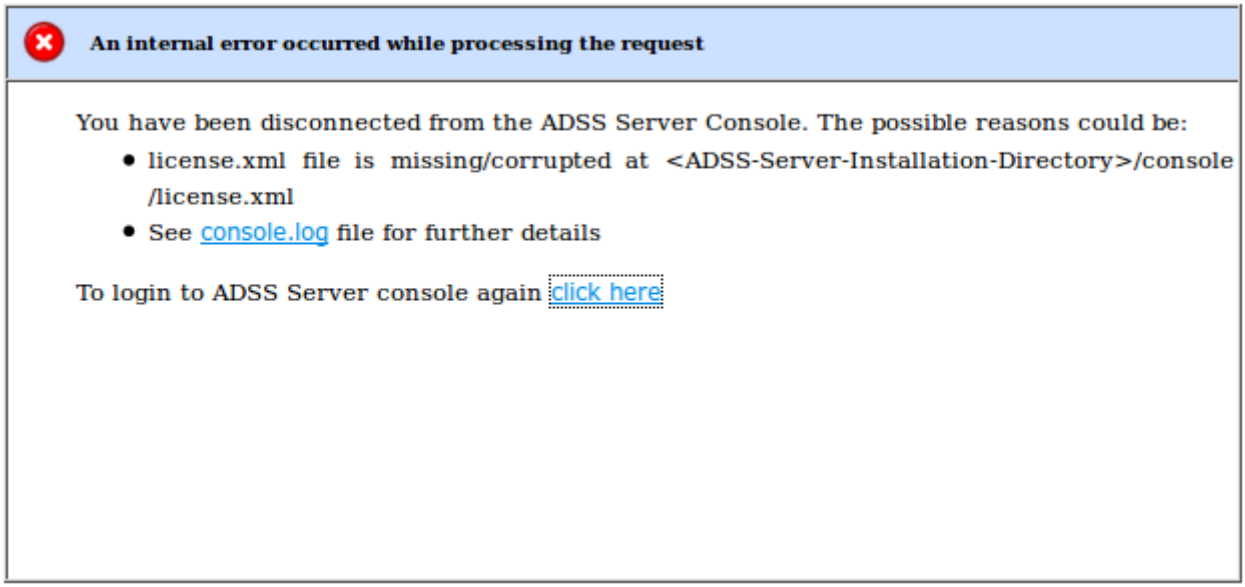


14. Reaching the end of the TP, we had to import the certificates into an email client and exchange signed emails between the group members(this was not possible at the moment of the prints). First we can see the imported certificate on *Mozilla Thunderbird*. The second image shows on the left the email sent from *Thunderbird* to another personal email of mine. On the right is the email client *Evolution* where I imported just the CA certificate.

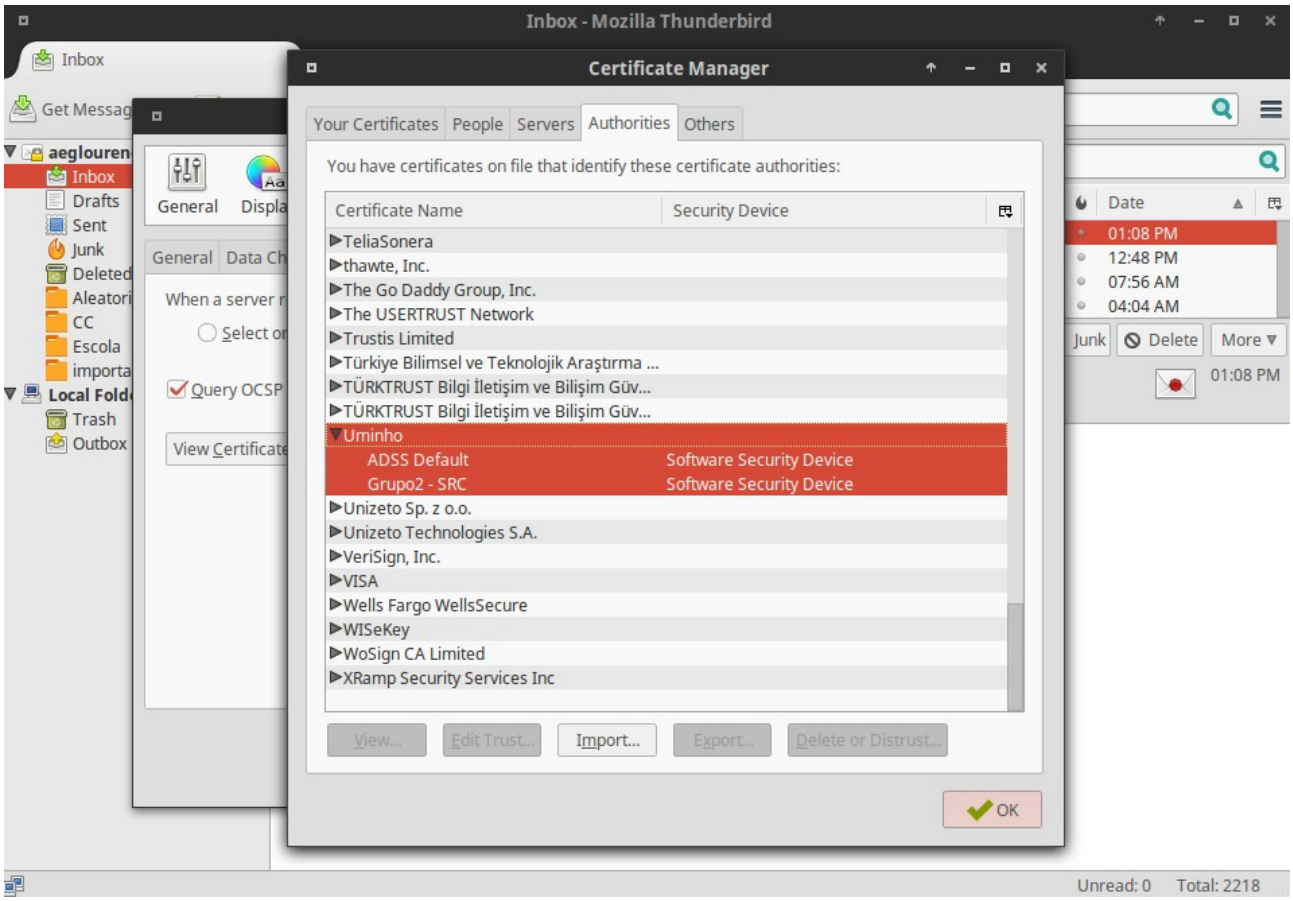




15. In this step it was asked to revoke a certificate. Unfortunately I was unable to access the adss server for the entirety of the day (26/03/2016). Hopefully I'll regain access to it and properly document it.



16. In this last part of the TP we had to exchange emails with colleagues from other groups. So, first we exchanged our Authority Certificates. In the first image it's highlighted both my group and the other one Authorities Certificates. In the second and third image we can see the received email and it's signature. The results on the other end were the same.



From jorge bastos
Subject **not a fake**
To Me

Reply | Forward | Archive | Junk | Delete | More

07:52 PM

hello