

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.

The screenshot displays the ADSS Server - Advanced Digital Signature Services home page. The page has a blue header with the Ascertia logo and navigation links. The main content area is divided into several sections:

- Product:** Product Name : ADSS Server - Advanced Digital Signature Services, Version : 5.0.0.4, Build : 5004.5000.190216.30921, Friendly Name : ADSS.
- License:** Company : University of Minho via DigitalSign, License Type : ADSS Server Evaluation Only, Contact Info : Henrique Santos, Contact Email : hsantos@dsi.uminho.pt.
- Database:** DBMS Name : PostgreSQL 9.2.7, DBMS Host / Port : localhost / 5432, Database Name : adss, Database User : adss_dbo.
- Operator:** Operator Name : MIETI-grp3, Operator Email : alunos@some.pt, Operator Role : Alunos, Login Time : 2016-03-23 17:02:28.
- Instance:** Host Machine : localhost.localdomain / 192.168.223.6, Operating System : Linux / 3.10.0-123.13.2.el7.x86_64, Core : Running, Console : Running.
- Services:** (Empty section with a traffic light icon).
- Alerts:** (Empty section with a sun icon).

The footer of the page contains the copyright notice: © Ascertia Limited. All rights reserved.

2. Since we are 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.

```
mangas@AL_LinuxMint ~/Desktop/src/tp3 $ openssl rsa -in privkey.pem -check
RSA key ok
writing RSA key
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAU6ghj45pK9k3xD36GiVe3EBMm298oL9MfMSZ4dp7AUcm0me
4rDbgCfgyfYmSKpBXI5tC6YG04Q/3PmRwQUVcQV4NM/wvNL0yPztKZhV250KToIu
9qVIOeagji7nj+Xk2M80PeV/UUB10hB2Idax0HYFE220tfW2++KszMSAKaVrzYgj
qXxEXXNCfnjTDF00y+fG99aeLCYXZelrv6F1qTl1jkRmBhjRNb76aUoSmoTpFqT0
0lR/9s8dqyjeE93asU02FQKRuQE0V4Bmas3LTISxyQZ3ZdgrJcI5j2G7UDZTtK/I
PsbhGJsZzGEsgyle3lYahU/2ZCsqm6aVVldjbQIDAQABAOIBAQC4nD/RckeegWkG
W/7Wx37XFZnM0tcc837FQj01dwnloAqIqV/nw/8a2EiFPeuMu3PoNgDDdLJ73SGG
dl8cc7+4K1RRdGNZUN9Vg8ooYSWBbz1WWIBCCWduc4EphzZM1YR3JlZGIIdNqQklj
5Ke/UiavmxhSH0oqKoga1bAcNjijgr7ABiN09nMnf8VQwzak/nu6iu4ngE0Fafpy
oNwUkayYPBYF0Qg/pXn4ae0o07a4RoYptjjq+bWxLps/Jftw5zaK6IKMtRlq6Zoq
5EioeqnZU/DmFhJLGeN4UdD42s0CDx/RXwezxD+dpY3f0TReWt0NchjVivX0R6h
606gypZFAoGBAOzEHSjSNQHRwhD0+w8cIJNQHNTx3NANc3YmVjsBu6bZ/vPeYVV
hyZRIjJG0MzV20gKopX0P90Bv65Xj45DZgFaC4gJWkGUFuE7QSVsLDf4EMRC7xvJ
PY0W0FARq93oTj3jbg9N+IYu3FEt2M8ZNZYuhvRZXC73eja/N+A2d8UjAoGBAMyV
iY+ekotU04YsMgBEMYV8xHk+452/8i3fkeBTnl5FBjlQ6lx4nL+dQ0x7Bn9Cnz+k
GwaRlNSIjucEmqa6RlgaII9anuEjQaEnW0wduR1sBb/snSPwAVaGPh4U3ZKYK06k
d5CkNCi/aU2mUtUxh0kL9uHIu2dlv+4TrXHPfSYvAoGAXWy1JNptWB5wuUgxmLC8
meR0vCgDvYTRPo+gV2orAhQIX/BqPxaUkaYKHfSDJ3ZqdIVdykbsIIVeIWkjmDs4
E0h7DF7EYoQQ0ycSfEZg3GTiGM9gkLJC6l3dMpsGejWkSf9n+loF6syq2s2Ac5e6
8VvCnMB2A4Jbkya44ZwcfokCgYA1hb0xyeRF/JuoBQx7ynesKSiLD8/TIyr/pdNu
Vk82FVSATlFKJtV0Gx+r9quHQX0E37Mop/+AJ8k+TWznJhSbxUS+V5LuChsS0clC
yPTr5aBHRGb+y7Z92pKJqSkb0SEx6j29m8Jr2U1+3XwRdWcLyc4f0i525hte9NRI
y1nNTwKBgQDWP3bbz+93RF4m9r9gP0baNr6Zt9/Fxho/Cz2imtgDxdddVQ6IAaTQ
2w0nTaANALHbzaP0veHz7lrTZtRL1x0JJYAbHHvTqHBVZyq82RJEokt2IDjInt7b
aYiuozuLoW+14ISv7R0Q7updTECnMeicD7CR9NLY2+qZRewLHFByIA==
-----END RSA PRIVATE KEY-----
mangas@AL_LinuxMint ~/Desktop/src/tp3 $ _
```

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:l8:9b: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/emailAddress=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.

Key Manager > Service Keys > New

New

Key Alias*: SRCGrupo3

Purpose*: Certificate/CRL Signing

Crypto Profile*: Software

Key Algorithm*: RSA

Key Length*: 2048

☐ Allow the private key to be exported later as PFX/PKCS#12 file

OK Cancel

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

Key Manager > Service Keys > Certificates > Create CSR/Certificate

General Details

Key Alias: SRCGrupo3

Certificate Template: Default Certificate/CRL Signing Template View Template

Certificate Alias*: SRCGrupo3-CA

Requested Certificate Details

Common Name*: ADSS Default +

Organization Unit: DSI +

Organization: Uminho +

Email: aeglourenco@hotmail.com +

Locality: +

Street Address: +

Postal Code: +

State: +

Country: Portugal +

Serial Number: +

Business Category: +

Note: Any field(s) left blank will not appear in certificate Subject Distinguished Name

Subject Alternative Name Details:

Alternative Name: rfc822Name +

Certificate Processing Details

☐ Use Local CA (as configured in Manage CAs Module)

☐ Use External CA

☒ Create Self-Signed Certificate

☐ Auto renew certificate

OK Cancel

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

Certificate Details

General

Path

Version : 3

Serial No : 1233c5cc615e0d3bb

Subject DN :

Common Name : ADSS Default
Organisation Unit : DSI
Organisation : Uminho
Email : aeglourenco@hotmail.com
Country : PT

Issuer DN :

Common Name : ADSS Default
Organisation Unit : DSI
Organisation : Uminho
Email : aeglourenco@hotmail.com
Country : PT

Signature Algorithm : sha256WithRSAEncryption

Validity :

From : 2016-03-25 14:29:50

To : 2021-03-25 14:29:50

Public Key : RSA (2048 Bits)

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:BA:B
2:14:D9:76:88:03:D4:EA:29:3D:D0:FA:CA:06:77:8E:3D:4C:FE:19:80:80:F2:C7:03:E5:A6:FD:BA:BD:28:6F:6F:0E
:A2:4E:6F:5B:E6:96:A4:F6:14:F6:49:C8:69:00:0F:E6:0F:77:3F:89:E6:DD:55:F3:79:57:41:A3:E0:46:03:67:8A:FC
:02:B7:89:13:DD:A3:6C:8F:F9:9A:ED:5D:3A:6A:29:B9:CC:4E:2D:AE:97:5A:41:E4:21:E8:1F:8D:F3:7A:07:A2:B2:
57:79:E1:62:44:34:E1:35:F5:6B:A8:6D:AE:DD:44:27:E4:79:30:EF:8E:BE:62:1C:B5:80:AD:65:19:97:22:F9:4F:B2
:95:BE:84:3C:75:7C:06:D7:DD:3F:B8:79:F6:4F:DF:7F:2F:65:84:76:C8:F1:09:04:55:AF:64:78:B6:4F:48:C5:C5:04
:85:3B:F6:98:97:22:D5:D9:23:D5:4E:C4:CE:74:F5:7F:54:E9:64:94:AC:0F:68:CB:60:0F:AD:C6:0F:E0:FF:8A:05:5
1:DD:70:92:74:C3:88:52:0E:42:B6:36:35:0C:1F:F1:B7:79:8A:5C:08:C8:F9:D4:6B:13:8E:0F:D4:29:FA:10:B7:05:F
8:54:6A:B9:21:8F:10:78:6D:65:65:46:6E:89:F8:44:D9:8E:07:02:03:01:00:01

Basic Constraints : Type=CA, PathLength=-1

Key Usage : cRLSign, keyCertSign

Authority Key Identifier : 89:1C:A1:19:F8:30:13:F2:8B:00:91:79:8F:69:B9:1A:2E:FB:18:DD

Subject Key Identifier : 89:1C:A1:19:F8:30:13:F2:8B:00:91:79:8F:69:B9:1A:2E:FB:18:DD

Thumbprint Algorithm : sha1

Thumbprint : I7Ib/ZRiWvYrLh/GV1IWJQ==

Save As

Close

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

Manage CAs > Configure Local CAs > New

CA Certificate Info

Status: Active
☐ Use as default CA
CA Friendly Name*: SRCGrupo3-CA
Description:
CA Certificate: SRCGrupo3-CA View Certificate

Note: The CA certificate must already have been generated/imported in the ADSS Key Manager with the purpose "Cert/CRL signing".

CRL Settings

CRL Validity Period*: 1440 (min)
☒ Generate and publish CRL automatically
CRL Publishing Period*: 240 (mins)
☒ Publish emergency CRL whenever a certificate status is changed
Hashing Algorithm: SHA256
CRL Publishing File Path: /var/www/html/certificados/SRCGrupo3-CA.crl Test
e.g. /dir/sample.crl

LDAP Settings

☐ Publish CRL in LDAP
☐ Publish Issued certificates in LDAP

Certificate Extensions

CDP Address (HTTP): http://e-tslab.dsi.uminho.pt/certificados
CDP Address (LDAP):
AIA Address (OCSP):
AIA Address (CA Cert):
Issuer Alternative Name OID (otherName): Value:

Certificate Validity Settings

If Issued Certificate Expiry Is Beyond CA's Certificate Expiry:
☒ Issue the certificate
☐ Use CA's expiry date/time
☐ Return an error

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

Manage CAs > Manual Certification

Manual Certification

Certificate Alias*:

Import PKCS#10*: cert.csr

☒ Use Local CA (ADSS Server inbuilt CA)

Certificate Template*:

CA Certificate*:

☐ Use External online CA

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

Manage CAs > Configure Local CAs > Issued Certificates (SRCGrupo3-CA)

Showing page 1 of 1

Order by:

	Certificate Alias	Valid From	Valid To	Source	Status
<input checked="" type="radio"/>	Antonio	2016-03-25 15:54:54	2017-03-25 15:54:54	Manual Certification	Active

d/mca/lca/managelca.do

Operator: MIETI-grp3

CA's [System Logs](#)

Manage CAs > Configure Local CAs > Issued Certificate

Showing page 1 of 1

	Certificate Alias	Valid From
<input checked="" type="radio"/>	Antonio	2016-03-25 15:54:54

Certificate Details

General Path

Version : 3

Serial No : 1187483e6b8b3cb02

Subject DN :

Email : aeglourenco@hotmail.com

Common Name : Antonio

Organisation : Universidade do Minho

Locality : Guimaraes

State : Braga

Country : PT

Issuer DN :

Common Name : ADSS Default

Organisation Unit : DSI

Organisation : Uminho

Email : aeglourenco@hotmail.com

Country : PT

Signature Algorithm : sha256WithRSAEncryption

Validity :

From : 2016-03-25 15:54:54

To : 2017-03-25 15:54:54

Public Key : RSA (2048 Bits)

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00: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:02:03:01:00:01

Basic Constraints : Type=End Entity

Key Usage : nonRepudiation, keyEncipherment, digitalSignature

Extended Key Usage : emailProtection

Thumbprint Algorithm : sha1

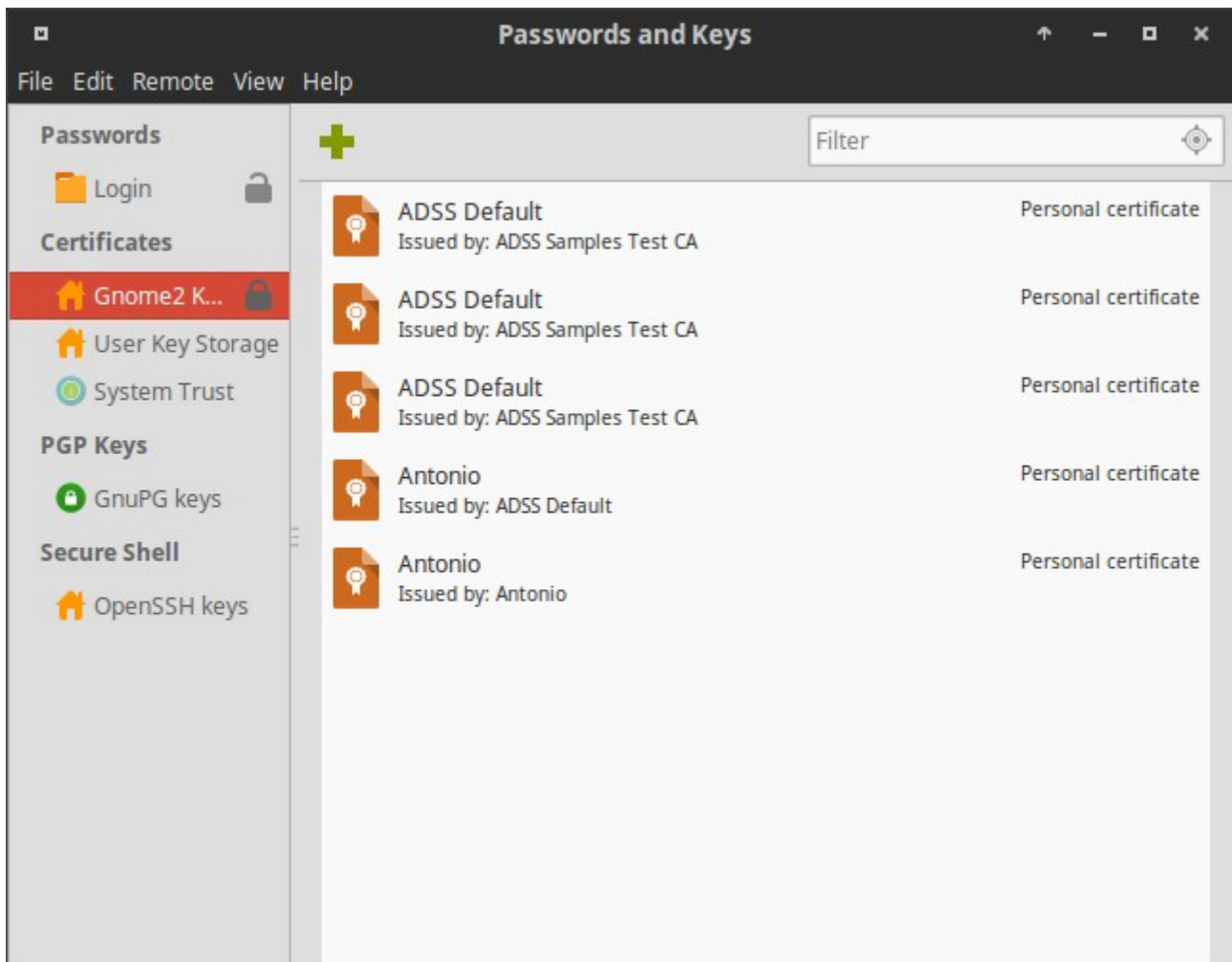
Thumbprint : IMGh/HZt683PZwonFX9NA==

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.

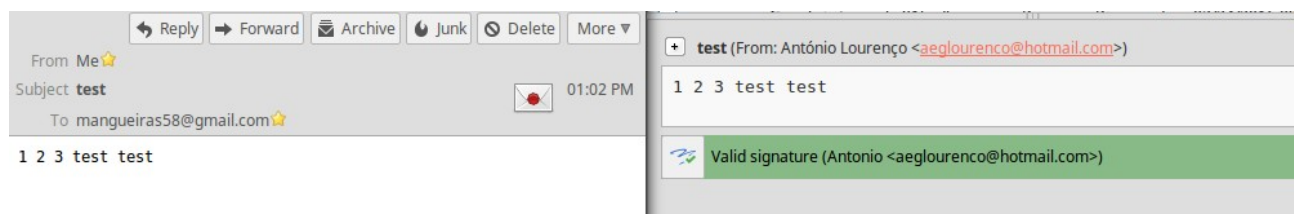
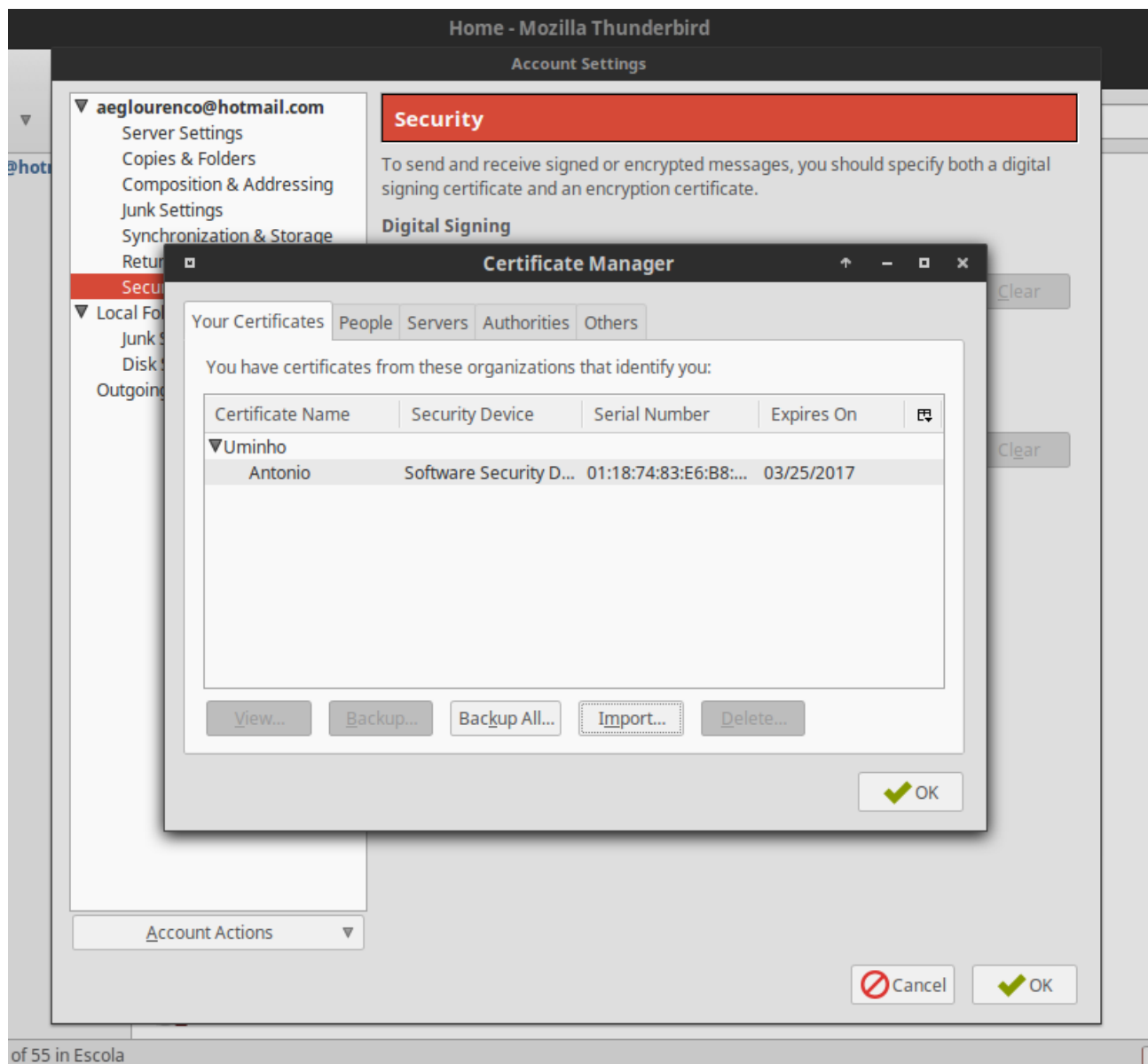
```
Terminal
mangas@AL_LinuxMint ~/Desktop/src/tp3 $ openssl x509 -inform der -in personalcertificate.cer -out percert.pem
mangas@AL_LinuxMint ~/Desktop/src/tp3 $ openssl x509 -inform der -in CACert.cer -out CACert.pem
mangas@AL_LinuxMint ~/Desktop/src/tp3 $ _

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 $ _
```

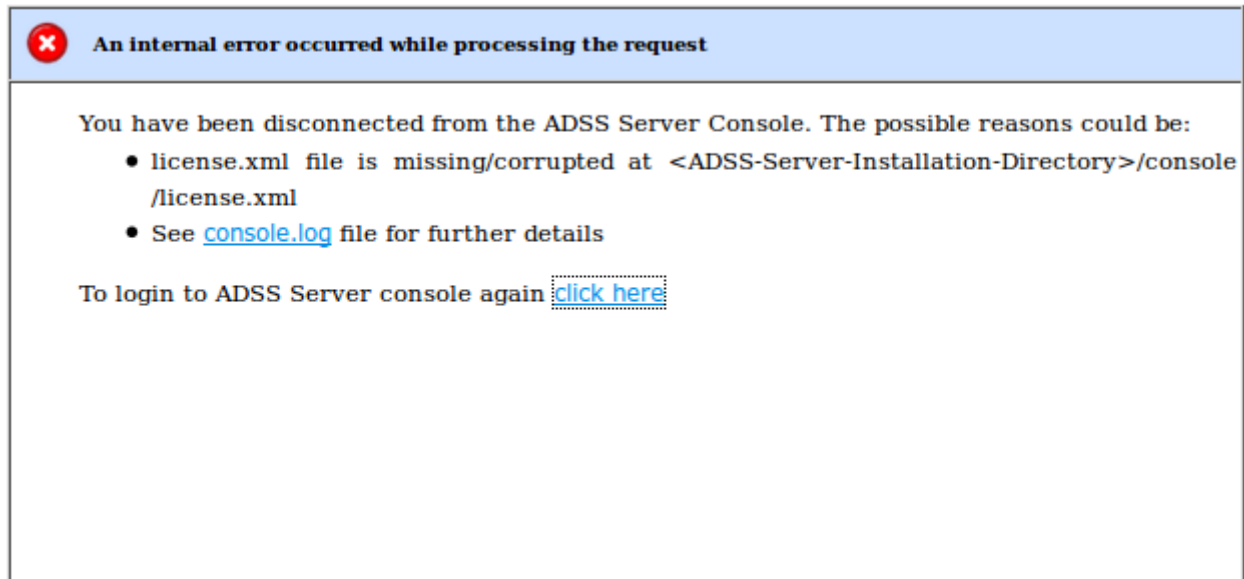
13. Now we had to import all of this certificates to the OS. Here we can see the program *Passwords and Keys* that manages the certificates imported.



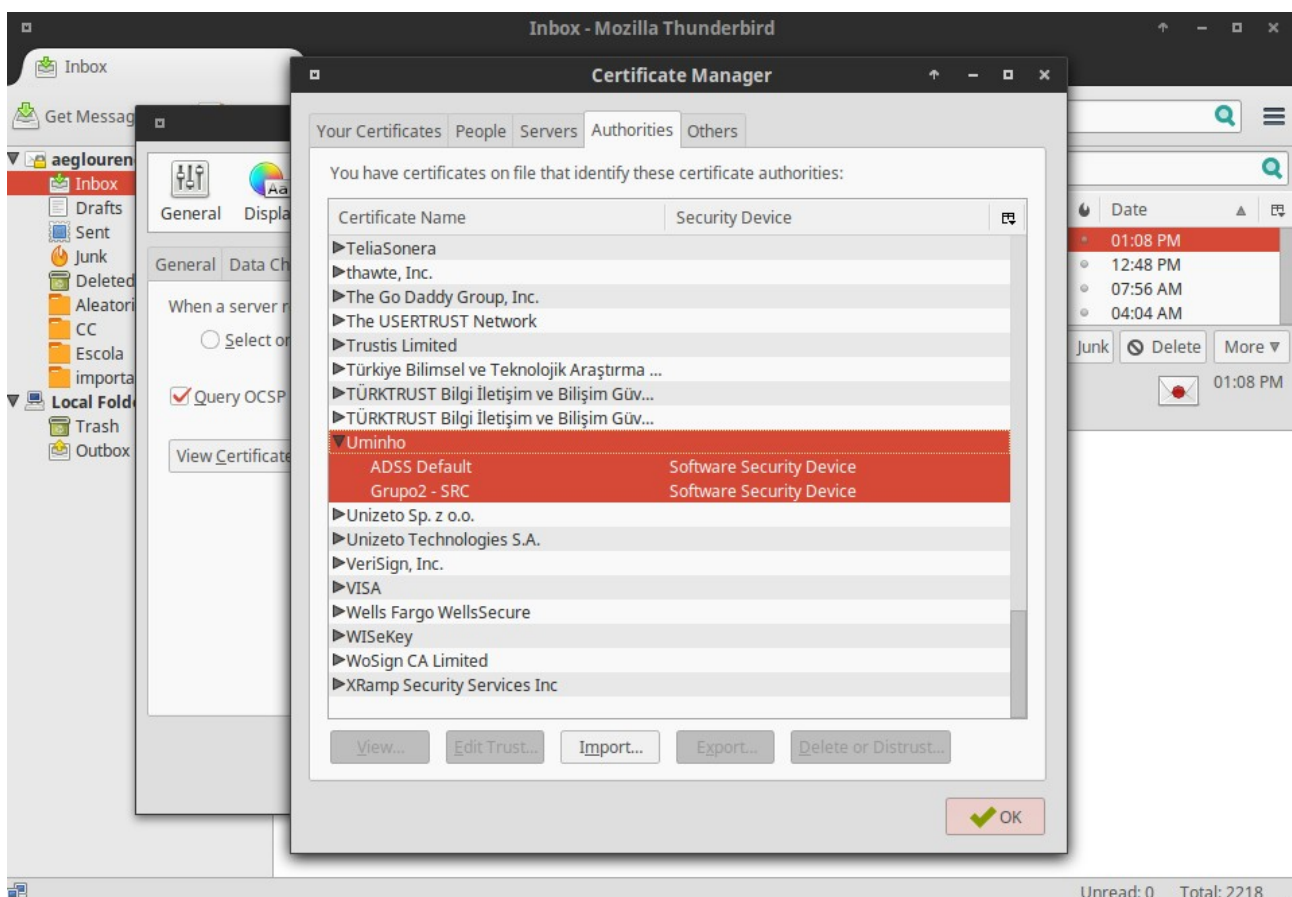
14. Reaching the end of the TP, we had to import the certificates into an email client and exchange signed emails between the group members (this was not possible at the moment of the prints). First we can see the imported certificate on *Mozilla Thunderbird*. The second image shows on the left the email 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

Inbox - Mozilla Thunderbird

Message Security

Message Is Signed
This message includes a valid digital signature. The message has not been altered since it was sent.

Signed by: Jorge Bastos
Email address: a68456@alunos.uminho.pt
Certificate issued by: Grupo2 - SRC

[View Signature Certificate](#)

Message Not Encrypted
This message was not encrypted before it was sent. Information sent over the Internet without encryption can be seen by other people while in transit.

OK