

Trabalho Prático 3 - Cifra, assinaturas, certificados e o ADSS

Gonçalo Pereira, José Silva, Matias Araújo, Miguel Costa, Nuno Vieira
a74413, a75280, a76234, a72362, a74014

17 de novembro de 2017

1 Logbook

Com a criação deste *logbook* pretendemos manter documentação de todos os passos tomados na realização de cada uma das alíneas do atual trabalho prático, especificando decisões tomadas e ilustrando o que foi visto aquando da resolução das mesmas.

1.1 Alínea 3

Após geração da chave privada com recurso ao comando `openssl rsa -in privkey.pem -check`, verificámos o seguinte estado da chave:

```
MINGW64:/c/Users/XoRtY/Desktop/SR
XoRtY@DESKTOP-BNUG8MI MINGW64 ~/Desktop/SR
$ openssl rsa -in privkey.pem -check
RSA key ok
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAs1ItcpE3CyMVuxnL607fWKTvpAimD+Ik1mM1gYqoRV7TYgpU
b1KcKqQ/7B2oyiFNCPub9G77sGJGHVnC5vqYtZxcEhQwkwl1t4YzveAcZMFk8iB3h
SfsbZWzyFaUvvgQxMRhFRyVwhKTWlKMyXsrH1Er0ZwzaPCRBjm70iaidpaqQuD
y0F9Af3F1Ke4uz86WkuysjxuZJiIVq+OTXteo25UaSNqqYDPwBe6yoYegcpzyBe1
dV2tLIauKxN/Q/+wr+UtVx8Jw+GnQgadbXncamDV2CiRpjpkA4c2m0ycFzJ/gpFS
KZ46tJkr7c6Q1e1U7QMFNprhSqQDEPmo+GVZHQIDAQABAoIBAA4HRMTstViqsv2D
JB+h6FkF9htoDc26TFV1Ri7fMRDUPUczNa23oVFeja3j0fY2RT1T+2MbSY8we3b4
tJ9Ekt4y0K5U3rdIkZ95xIFxC0zJ3ghr/jAq0EBB+NHm/N5JnwHwR0sYaFgIKTV
PSZwvad+2Uu4/ftybzUymYY5IDXefHftvU1w3XC4GncxTV/JrCUzAlYewGqqHsmg
hEv1CAA0t/lrVsMPtaN5TtEIss/oPudQMnyDpy/VTGx1hdvJ0CN7i4vQr0IjNwqC
YoMhioZwMwqKCHU9NegURKJgtK4RQDsRhp6rFcZK98Z2jNN+hgex1x/eGAG/8frP
QqZFD0UCgYEA7no+19w1H8SP8M+96l2qatt3i6URL1tbQ713VKwQbLYzrBbTVmI
jAzyRwtdaA1dpIBxKwyBhqwhMZStkFEg3UK2EDm4vmhSX4QThnfl5RjL7xvL0BB1
yIepby0oV2H0hUkFUsXmRWATGGLNxS1V23Tn7Gf1Nzuq7XswjuflZcCgYEAwH8Z
LC+WOHxqbTIs752XaRE7NyPh2UF8TywQak7SuvCkUe+KiITBwsJUB8FAOUuth9l+
8Yf2MyKowcIXaMRU6weJ8CiF2PkSF6vnJ6k7PX/KnDN6Hb7kFJxOMjdhnR0Ju+Tm
cswKbBLSzrctK6QFMVtd6+evjvIHpGmevFxrnEsCgYEAx18ABuWthR+JzyN+fn9N
x/6/ltc7Y+wQgrN1fhjkgl5XX6Dk0+fUvNHEyfd066aw8QRImFreNr11590Kvyp0
NUa+exYms1j39M6wnCyvE5WwUUhKE9C+hSGLSbg37f36EVKHVh3vXpYxKqop/ySNj
mhND8rXw21dSwc/ABzftP0UCgYASV8yjiEFTT/BmgdoKec0rtyqq30pBTF4RUcM
wUAZajbuS9oywb/fCyEauayKCSkXceWrlF3kj4fvNrSOWi8Rwl2Nkf73JvzPXqUf
RWQMvzGqYs1fLkKdQEVXigW+N/cmFXBsPf88Py1roU7fmriX9HH1ueUjxPJve1UR
8+iZMwKBgQDik2y1crgRm/yva10qIVbuUxQy7HFMwYz1txqzo1jKm817qWmDsN1+
Wx6R6mVqtYSPeVw524kbDzxkpaHkX5AEqK21/HilGGsWE23/81+XlGchMIAxEYrg
dk1K0wsAwLPITCsZodficUGqBGHC0XwFPALNnsFdvODy+E4h1DfIRA==
-----END RSA PRIVATE KEY-----
writing RSA key
XoRtY@DESKTOP-BNUG8MI MINGW64 ~/Desktop/SR
$
```

Comprovando-se que estaria funcional.

1.2 Alínea 4

Gerando-se o pedido de certificado através da execução de `openssl req -text -noout -verify -in cert.csr`, obtivemos a seguinte resposta:

```
MINGW64; c:/Users/XoRtY/Desktop/SR
An optional company name []:

XoRtY@DESKTOP-BNUG8MI MINGW64 ~/Desktop/SR
$ openssl req -text -noout -verify -in cert.csr
Certificate Request:
Data:
  Version: 0 (0x0)
  Subject: C=PT, ST=Some-State, L=Braga, O=Internet Widgits Pty Ltd, CN=miguel/emailAddress=miguel.m.costa15@gmail.com
  Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    Public-Key: (2048 bit)
    Modulus:
      00:b3:52:2d:72:91:37:0b:23:15:bb:19:cb:e8:ee:
      df:58:a4:ef:a4:08:a6:0f:e2:24:d6:63:25:81:8a:
      a8:45:5e:d3:62:0a:54:6e:50:8a:a9:0f:fb:07:6a:
      32:88:53:42:3d:46:fd:1b:be:ec:18:91:87:56:70:
      b9:be:a6:2d:67:17:04:85:0c:24:c2:5d:6d:e1:8c:
      ef:78:07:19:30:59:3c:88:12:61:49:fb:1b:65:6c:
      f2:15:a5:2f:8a:04:31:31:18:45:ad:16:15:c2:12:
      93:58:b9:0c:23:25:d2:ac:7d:44:af:46:56:cd:a3:
      c2:44:18:e6:ec:e8:9a:89:da:5a:a9:0b:9d:cb:47:
      fd:01:fd:c5:94:a7:b8:bb:3f:3a:5a:4b:b2:b2:3c:
      6e:64:98:88:56:af:8e:4d:7b:5e:a3:6e:54:69:23:
      6a:a9:80:cf:c0:17:ba:ca:86:1e:81:ca:73:c8:17:
      a5:75:5d:ad:2c:86:ae:2b:13:7f:43:ff:b0:af:e5:
      2d:57:1f:09:c3:e1:a7:42:06:9d:6d:79:dc:6a:60:
      d5:d8:28:91:a6:3a:64:6b:87:36:9b:4c:9c:17:32:
      7f:82:97:d2:29:9e:3a:b4:99:2b:ed:ce:90:d5:e9:
      54:ed:03:05:36:9a:e1:4a:a4:03:10:f9:a8:f8:65:
      59:1d
    Exponent: 65537 (0x10001)
  Attributes:
    challengePassword :cenas123
  Signature Algorithm: sha256WithRSAEncryption
    15:ed:ff:ab:62:27:47:3a:2b:bb:c4:e3:47:93:b4:7f:17:4f:
    95:cf:79:39:f5:fd:ed:ed:f1:ab:16:cd:d6:6d:7f:bf:3d:50:
    43:2f:ee:6c:5d:6d:97:11:98:41:6b:bd:04:8d:e3:5e:68:63:
    43:75:d3:a6:03:04:6c:e9:99:52:94:a5:a9:25:4f:14:ee:0a:
    80:7c:7e:a2:95:68:d3:1e:fa:19:94:b6:93:ad:86:1c:fb:6a:
    da:96:3f:0f:81:9e:62:ba:e9:32:b9:21:3d:81:29:18:a9:ac:
    a7:9e:91:95:16:c4:23:34:ec:6e:aa:c9:e3:d1:bf:d7:70:96:
    0b:f8:59:a1:56:e2:d1:3d:cd:5d:c2:07:8c:cb:87:45:55:3d:
    75:48:ed:e1:17:a2:a8:10:a2:fa:8e:6b:4b:cc:d9:a9:2f:99:
    65:2a:6d:41:6d:77:b8:ac:93:23:9e:02:4c:ef:f6:0d:0a:03:
    a9:79:82:27:48:2e:c1:7d:5d:bf:5e:6b:7e:b5:19:87:4f:6f:
    48:50:46:da:64:6c:ec:53:75:6e:3c:cc:8e:ca:0c:f9:bd:30:
    3c:69:9d:22:e1:b9:11:25:1e:d9:38:aa:0d:42:c5:52:a7:6a:
    c7:15:7d:46:18:e1:01:aa:2c:3e:0c:06:8b:6f:3f:62:ad:15:
    14:c6:24:41
verify OK

XoRtY@DESKTOP-BNUG8MI MINGW64 ~/Desktop/SR
$
```

Na qual se pode verificar que se encontra em estado OK.

1.3 Alínea 7

Para efeitos de registo, ter-se-á tirado o seguinte *print screen*, com os parâmetros do *template* devidamente preenchidos:

General Details

Key Alias: SR-grp3-new

Certificate Template:
Default Certificate/CRL Signing Template
View Template

Certificate Alias*:
SR-grp3-new-CA

Requested Certificate Details

Common Name*: ADSS Default

Given Name:

Surname:

Title:

Organization Unit: DS

Organization: Uminho

Organization Identifier:

Email: miguel.m.costa15@gmail.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


1.4 Alínea 8


As propriedades do certificado, explícitas no ADSS, serão as seguintes:


Certificate Details

General


Path

 **Version :** 3


 **Serial No :** 0092028c5f4dcabc01322f25e5ac9366a364821bf5

 **Subject DN :**


Common Name : ADSS Default
Organisation Unit : DSI
Organisation : Uminho
Email : miguel.m.costa15@gmail.com
Country : PT


 **Issuer DN :**


Common Name : ADSS Default
Organisation Unit : DSI
Organisation : Uminho
Email : miguel.m.costa15@gmail.com
Country : PT

 **Signature Algorithm :** sha256WithRSAEncryption


 **Validity :**


 *From :* 2017-11-16 15:43:52


 *To :* 2022-11-16 15:43:52


 **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:
:82:01:01:00:82:DF:9E:4D:E6:B1:25:B5:85:F0:07:37:1A:43:FD:2C:B7:18:5E:81:AF:25:77:E3:B
E:92:0A:76:A8:24:54:4D:9E:B9:E3:1E:38:79:E8:05:72:8E:C4:74:97:FE:B6:A5:1F:80:8C:66:33:
10:E2:84:F4:66:06:8C:83:76:EA:E7:77:B8:56:5D:25:FF:C4:16:D3:77:2E:33:9E:2B:9C:44:DD:F
C:46:D0:38:C3:9C:9A:70:A3:A4:90:98:93:41:4B:1B:71:4E:37:DC:74:42:49:94:0C:C7:BB:68:ED
:A2:1F:94:67:C4:AE:D7:C0:9D:13:03:0D:EB:67:50:86:B3:83:FB:B8:EE:EC:62:36:7E:3E:AE:6E:
A8:63:88:18:66:ED:D8:FB:9E:6E:33:7F:B7:71:71:5E:DB:74:E4:99:FC:B0:0B:27:A3:E2:9C:C9:6
C:C7:01:60:34:AB:48:0F:EB:E7:1E:28:6A:76:22:F2:D5:EA:C7:FB:9D:22:CF:A8:76:6C:54:E0:77
:8F:6A:96:C6:CA:74:6A:1D:82:4A:ED:1B:68:B1:B6:6D:AD:2A:66:1E:5A:E7:38:25:17:0A:C9:56:
D7:5F:4E:A1:CC:1C:7C:43:54:73:00:DC:40:8D:FB:47:0A:59:3E:ED:F5:0B:32:D6:DE:4E:00:CA: //


 **Basic Constraints :** Type=CA, PathLength=-1

 **Key Usage :** cRLSign, keyCertSign

 **Authority Key Identifier :** B2:60:BD:0E:AC:77:99:E8:10:4B:A7:B5:5C:F1:2B:B7:D4:4C:9F:C4 //

 **Subject Key Identifier :** B2:60:BD:0E:AC:77:99:E8:10:4B:A7:B5:5C:F1:2B:B7:D4:4C:9F:C4 //

 **Thumbprint Algorithm :** sha1

 **Thumbprint :** uQnA9jC9Iu5APzzk5oQGmA==

1.5 Alínea 9

Para geração do CA, foram tomados os seguintes passos:

Manage CAs > Configure Local CAs > SR-grp3-new-CA

CA Certificate Settings

Status: Active

☐ Use as default CA

CA Friendly Name*: SR-grp3-new-CA

Description:

CA Certificate: SR-grp3-new-CA

View Certificate

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

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

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:

CRL Settings

CRL Validity Period*: 1440 (min)

☒ Generate and publish CRL automatically

CRL Publishing Period*: 120 (min)

☒ Publish emergency CRL whenever a certificate status is changed

Hashing Algorithm: SHA256

CRL Publishing File Path: /var/www/html/certificados/ficheiro-grp3.crl

Test

e.g. /dir/sample.crl

LDAP Publishing Settings

☐ Publish CRL in LDAP

☐ Publish issued certificates in LDAP

Não esquecendo a ativação da geração dos *logs CRL*:

System Logs > Event Logs > CRL Publishing

Event: CRL Publishing

Module: Manage CAs

Sub Module: Configure Local CAs

Occurred At : 2017-11-17 10:58:38.538

Status : Information

Event Log Details

CRL generated and published for 'SR-grp3-new-CA' successfully

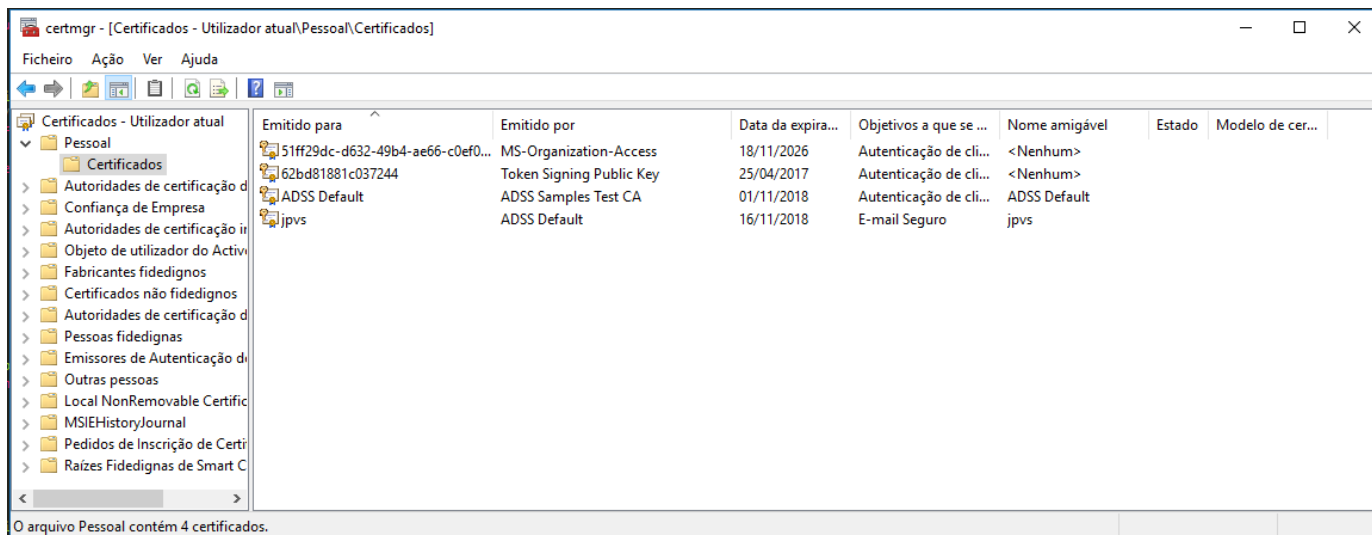
1.6 Alínea 11

Após verificação dos certificados emitidos, pudemos reparar que não existiam nenhuma discrepâncias, sendo que os certificados terão sido emitidos com relativa normalidade, tal como visto no seguinte *print screen*:

	Certificate Alias	Valid From	Valid To	Source	Status
<input checked="" type="radio"/>	nuno	2017-11-16 16:30:05	2018-11-16 16:30:05	Manual Certification	Active
<input type="radio"/>	Maitas	2017-11-16 16:12:44	2018-11-16 16:12:44	Manual Certification	Active
<input type="radio"/>	jose	2017-11-16 16:08:59	2018-11-16 16:08:59	Manual Certification	Active
<input type="radio"/>	miguel	2017-11-16 15:50:19	2018-11-16 15:50:19	Manual Certification	Active

1.7 Alínea 13

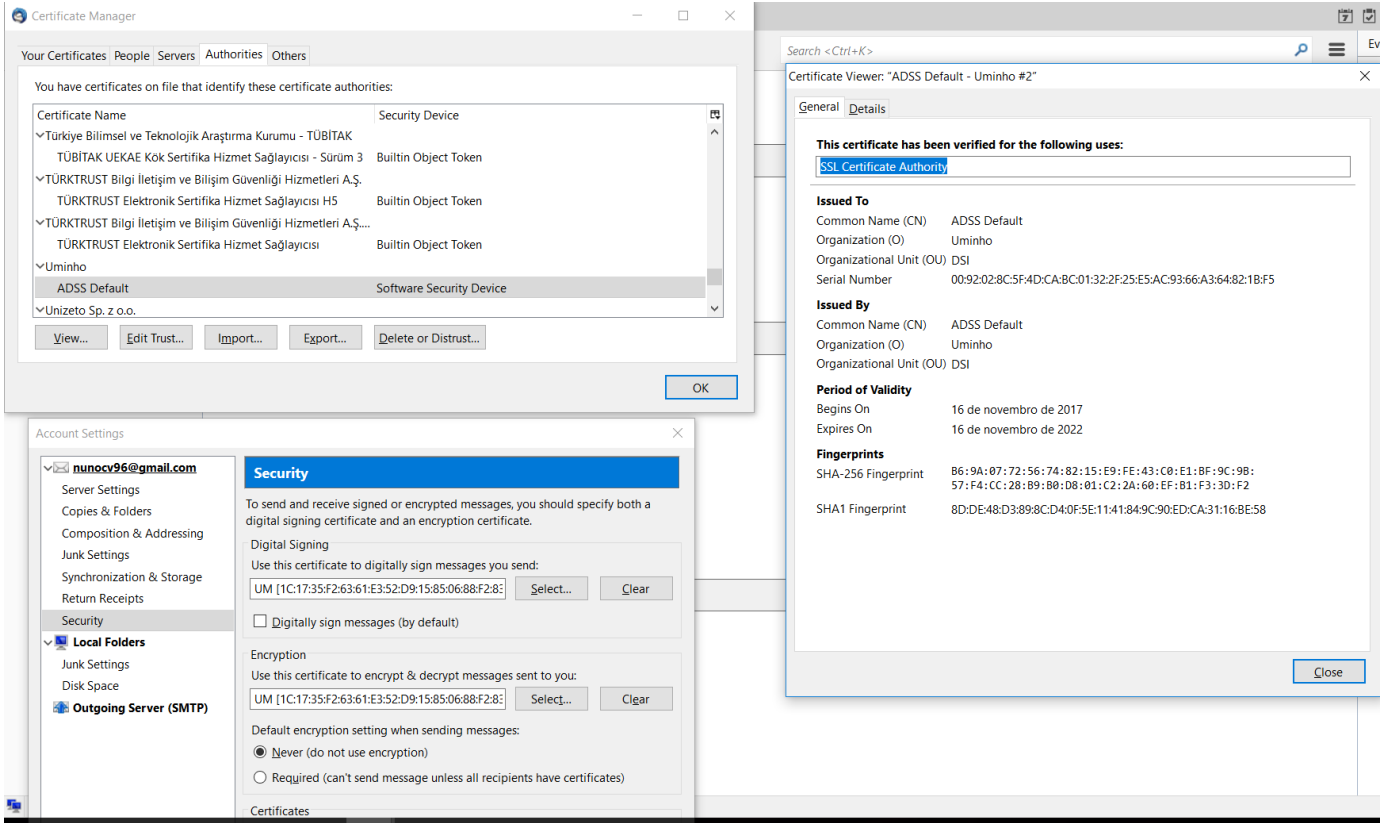
Após instalação de todos os certificados públicos, pudemos confirmar que a localização dos mesmos seria a da seguinte imagem:

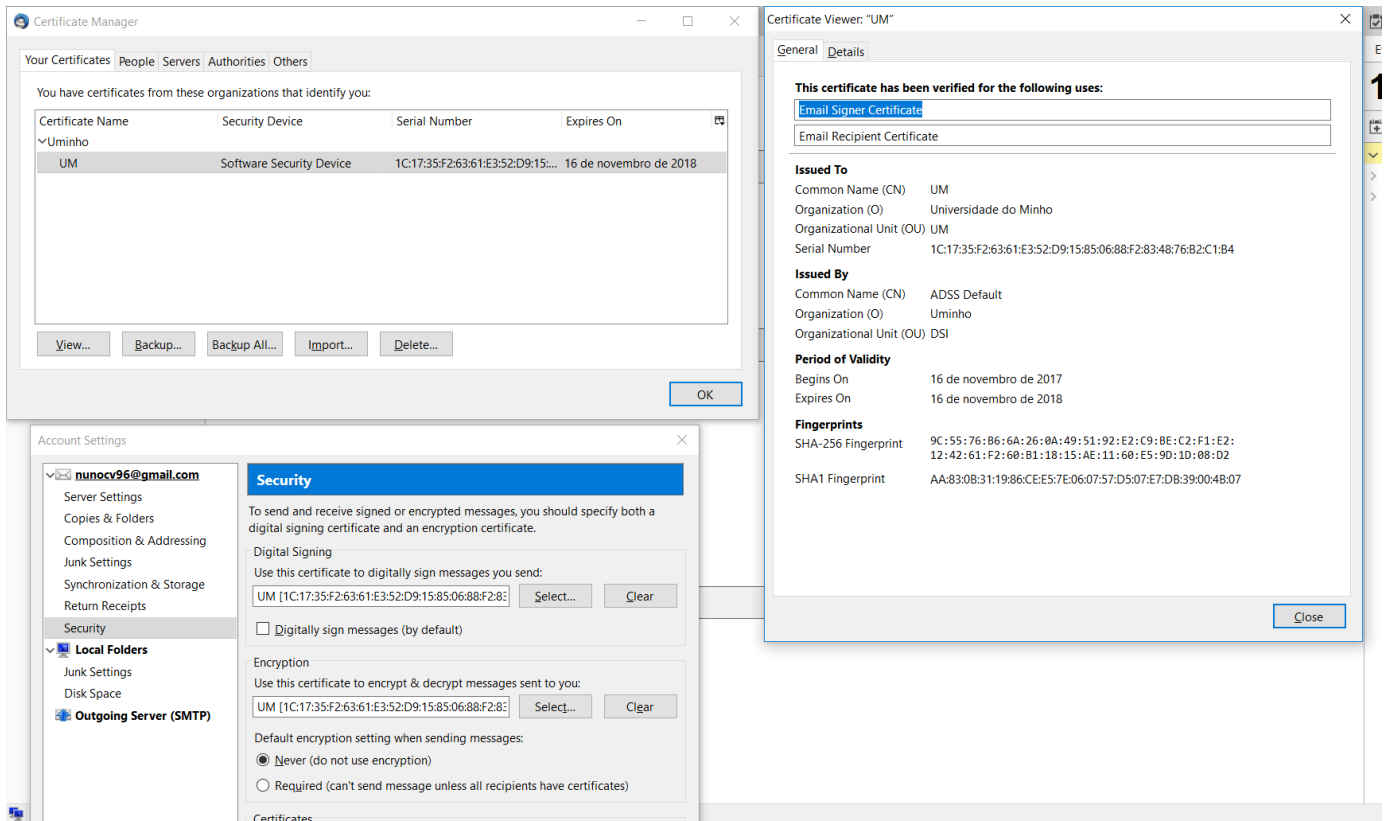


Como, no nosso caso, o **Windows** não terá reportado quaisquer anomalias, não terá sido necessário o registo da validação forçada por parte do sistema operativo.

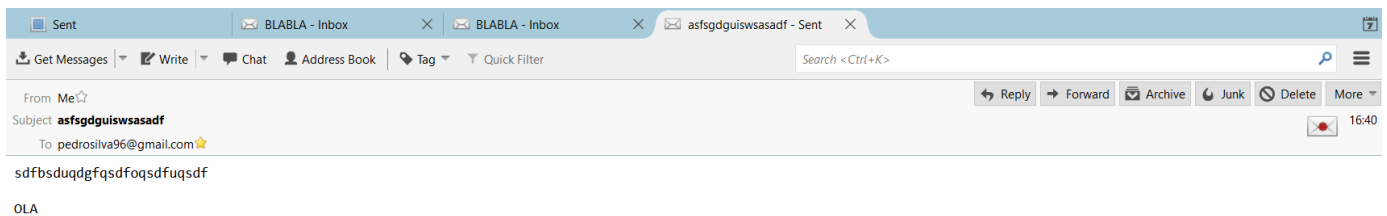
1.8 Alínea 14

Nesta alínea precisamos de instalar os certificados de autorização e a assinatura na nossa aplicação de cliente de email, Thunderbird. Nas duas figuras seguintes mostramos a sua instalação e a sua verificação em como se encontram instaladas.

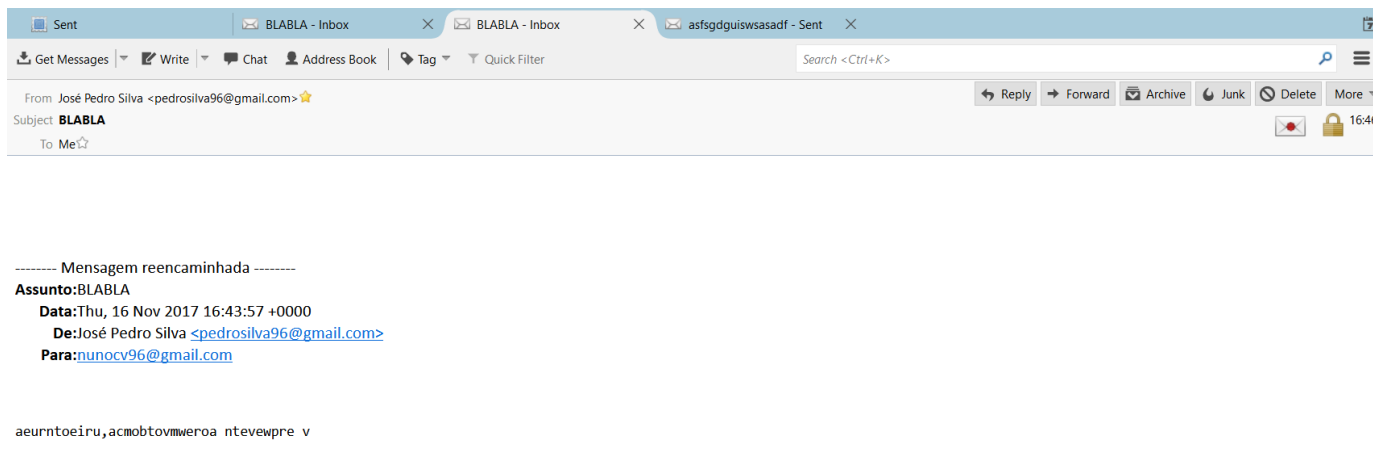




Reparamos que em antes de enviar um *e-mail* cifrado, tivemos que fazer um *handshake* para que pudéssemos de seguida cifrar todas as seguintes mensagens.



Por fim enviamos mensagens cifradas entre nós.



1.9 Alínea 15

Acedendo ao separador de gestão de CAs, seguido da opção de configuração de CAs locais e da opção de certificados emitidos, verificámos o seguinte:

	Certificate Alias	Valid From	Valid To	Source	Status
<input checked="" type="radio"/>	nuno	2017-11-16 16:30:05	2018-11-16 16:30:05	Manual Certification	Active
<input type="radio"/>	Maitas	2017-11-16 16:12:44	2018-11-16 16:12:44	Manual Certification	Active
<input type="radio"/>	jose	2017-11-16 16:08:59	2018-11-16 16:08:59	Manual Certification	Active
<input type="radio"/>	miquel	2017-11-16 15:50:19	2018-11-16 15:50:19	Manual Certification	Active

Após a revogação de um dos certificados, deparámo-nos com o seguinte:

	Certificate Alias	Valid From	Valid To	Source	Status
<input checked="" type="radio"/>	nuno	2017-11-16 16:30:05	2018-11-16 16:30:05	Manual Certification	Active
<input type="radio"/>	Maitas	2017-11-16 16:12:44	2018-11-16 16:12:44	Manual Certification	Active
<input type="radio"/>	jose	2017-11-16 16:08:59	2018-11-16 16:08:59	Manual Certification	Revoked
<input type="radio"/>	miquel	2017-11-16 15:50:19	2018-11-16 15:50:19	Manual Certification	Active

De modo a confirmar a revogação, consultámos os *logs* CRL, nos quais pudemos verificar que a revogação teria ocorrido com sucesso:

Total Records: 1
CA Friendly Name: SR-grp3-new-CA (Configured Local CA)
CRL Number: 2
This Update: 2017-11-17 11:03:16
Next Update: 2017-11-18 11:03:16

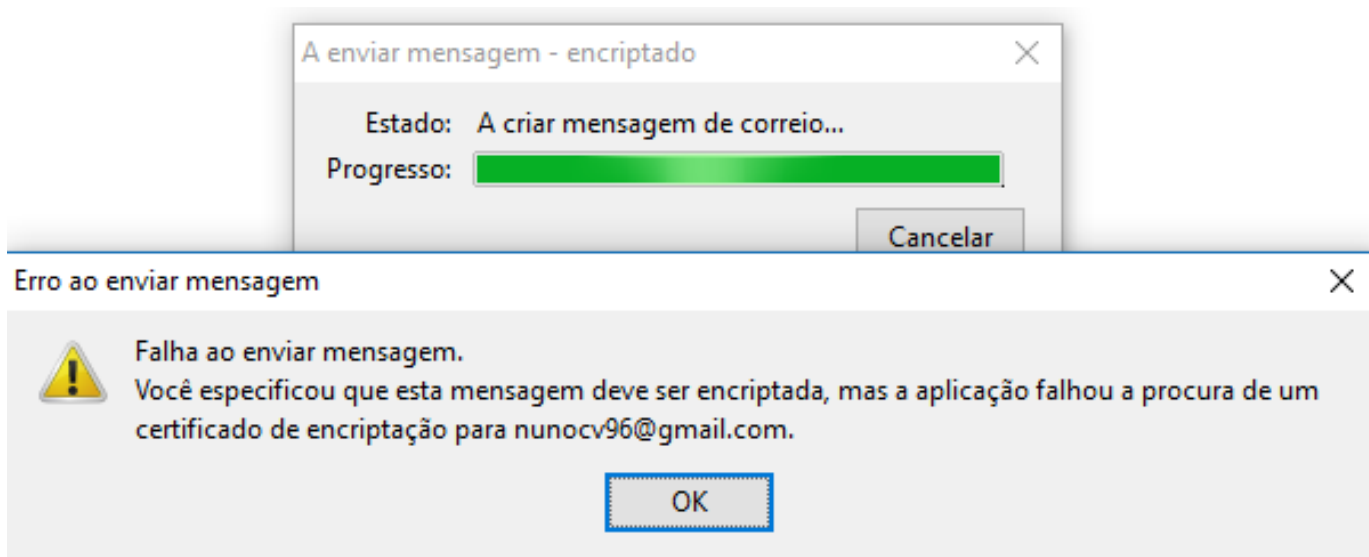
Showing page 1 of 1

Order by: Revoked At Descending Clear Search Search					
ID	Serial No. {hex}	Revoked At	Invalidity Date	Revocation Reason	Hold Instruction Code
2	1959229aa3686e9c64c6ed44183d508c91c23056	2017-11-17 11:03:15	2017-11-17 11:01:01	[0] Unspecified	N/A

Back to View CRL

Como primeiro teste, decidimos enviar um email entre nós, no qual constatamos que o email foi enviado e encriptado à mesma, sendo o certificado revogado.

Só não foi possível encriptar o email quando o destinatário removeu o certificado manualmente, como se pode comprovar na imagem seguinte:



Após a tentativa de encriptar, enviamos sem encriptação e o e-email foi enviado e recebido com assinatura, quando esta foi revogada.

1.10 Alínea 16

Como não nos foi possível estabelecer qualquer interação entre o nosso grupo e outro grupo prático, não pudemos catalogar qualquer relação de confiança com um diferente grupo TP. Porém, e entre os membros do nosso grupo, foi

possível verificar que apenas existiriam relações de confiança entre os membros cujo certificado estaria explícito no ADSS, sendo que, propositadamente, um dos membros não terá criado certificado (para motivos de teste), confirmando a eventual situação.