



Universidade do Minho
Escola de Engenharia

MESTRADO INTEGRADO EM ENGENHARIA DE TELECOMUNICAÇÕES E INFORMÁTICA

SEGURANÇA EM REDES DE COMPUTADORES

CIFRA, ASSINATURAS, CERTIFICADOS E ADSS

TRABALHO PRÁTICO Nº3

Grupo 9:

Cláudia Cristiana de Amorim Dias - A78232

David José Ressurreição Alves - A79625

Guimarães, 29 de Março de 2019

Índice

1	Introdução	4
2	Inicialização	5
2.1	Gerar par de chaves RSA	5
2.2	Verificação das chaves privadas RSA	6
2.3	Gerar um pedido de certificado X.509	8
2.4	Certificado auto-assinado	10
3	Servidor ADSS	11
3.1	Gerar par de chaves RSA	11
3.2	Gerar certificado da Autoridade de Certificação	12
3.3	Gerar certificados assinados pela CA	14
3.4	Gerar Certificados PKCS12	16
3.5	Instalação dos certificados	17
3.6	Assinar digitalmente documento	19
4	Troca segura de mensagens	20
4.1	Troca de mensagens usando certificados X.509	20
4.2	Troca de mensagens usando certificados PGP	23
4.3	Troca de mensagens entre grupos	25

Lista de Figuras

1	Criação de um par de chaves RSA.	5
2	Verificação da chave privada criada pela Cláudia.	6
3	Verificação da chave privada criada pelo David.	7
4	Efetua pedido de certificado.	8
5	Verifica pedido de certificado da Cláudia.	9
6	Verifica pedido de certificado do David.	9
7	Criação de um certificado auto-assinado pela Cláudia.	10
8	Criação de um certificado auto-assinado pelo David.	10
9	Criação de um par de chaves.	11
10	Criação do certificado auto-assinado da CA.	12
11	Consulta do certificado da CA.	13
12	Criação de um certificado para cada elemento do grupo.	14
13	Criação de um certificado para cada elemento do grupo.	14
14	Lista de certificados assinados pela CA.	14
15	Consulta do certificado <i>Claudia_novo</i>	15
16	Consulta do certificado <i>David_novo_certificado</i>	16
17	Criação do ficheiro no formato PKCS12(Cláudia).	17
18	Criação do ficheiro no formato PKCS12(David).	17
19	Definição do certificado da CA como certificado de raíz.	17
20	Definição dos certificados de cada elemento como certificados de confiança.	18
21	Configuração do cliente de <i>e-mail Thunderbird</i>	18
22	Assinatura de um documento.	19
23	Envio de uma mensagem assinada.	20
24	Receção da mensagem assinada.	21
25	Resposta assinada à mensagem anterior.	21
26	Receção de uma mensagem assinada e encriptada.	22
27	Receção da mensagem encriptada e assinada.	22
28	Lista de chaves PGP.	23
29	Envio de mensagem assinada e encriptada.	23
30	Impossibilidade de decifrar.	24
31	Decifra e verifica assinatura.	24

32	Verificação da assinatura.	25
33	Receção da mensagem encriptada e assinada pelo Grupo 8.	26

1. Introdução

No contexto da unidade curricular de Segurança em Redes de Computadores, foi-nos pedido que implementássemos conceitos aprendidos nas aulas teóricas, mais especificamente os relacionados com a criação e utilização de certificados X.509, o funcionamento das autoridades de certificação e dos ADSS, bem como a utilização de OpenPGP e S/MIME em comunicações de correio eletrónico seguras. Para demonstrar o resultado do nosso trabalho foi-nos pedido redigir o presente *logbook*, no qual será possível de forma sucinta, mas objetiva, representar a elaboração das várias etapas do trabalho-prático. Para a implementação deste trabalho-prático, usaram-se sistemas operativos Linux (Kali Linux e Ubuntu).

2. Inicialização

Tal como pretendido, instalámos nos nossos computadores (mais concretamente, nos nossos *web-browsers*) o certificado disponibilizado pelo docente, para o nosso grupo, de modo a podermos usar o servidor ADSS.

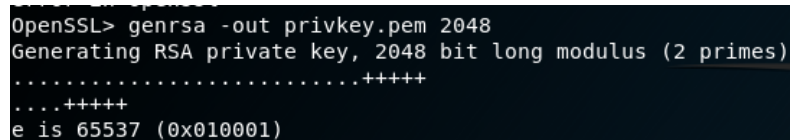
De seguida, procedemos à criação do par de chaves(públicas e privadas), bem como à sua respetiva verificação.

2.1. Gerar par de chaves RSA

Este procedimento foi executado por todos os elementos do grupo.

Tem como objetivo gerar um par de chaves RSA para posteriormente serem agregadas aos vários certificados, sendo assim úteis para assinar e cifrar dados.

- `openssl genrsa -out privkey.pem 2048`



```
OpenSSL> genrsa -out privkey.pem 2048
Generating RSA private key, 2048 bit long modulus (2 primes)
.....+++++
....+++++
e is 65537 (0x010001)
```

Figura 1: Criação de um par de chaves RSA.

2.2. Verificação das chaves privadas RSA

De modo a verificar o bom estado das chaves privadas, ambos os elementos do grupo verificaram as suas, de acordo com o seguinte comando:

- *openssl rsa -in privkey.pem -check*

```
OpenSSL> rsa -in privkey.pem -check
RSA key ok
writing RSA key
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAwmra5slEzx4REUv8zCfethvBjrPMrBV+D2WIGMa5pHQVb16+
3QQJd7AysW6u7iIHe57dXxYy/lBsXRwWv08e1FmFHUnoEYqzlfh036z0w0Q/XzRd
YVGWeg1AHUiqx20TexVoTeu/juNyw8t5TH8z0cAcnWI+TSs8CdPPTXCgflveWPTP
upeSH2MJ+hTi4l3qlfEoFpHxXUAu9JEtbaNCsw73EKzskuW3FY+y6Mxft+khpo05
nNntitiuasEQ0P3XlTjnZ3Kr9bugIvu70RR75MeA6NpdSzvTg2UYVbXFUzhCpPrd
ETNnx2DQVckuWhz8vn7gKSad7v0NkZ979nHV7QIDAQABAoIBAQCcZTkSznX750Pz
lh0WXjxaypmiIiFTjTaLTDHfPH26PWfAEZeYU9cJ4U0SrucpyVYbrACIrWL4Edoa
TK497l3uLNTwar006M7upYFNjcYEhZg1DfrQfsF+DYq2A+7d1sydBuuRQ0QlvfJk
bXP03x5mJpTeRlm32j/B6BGrSh7Rhc62zsa57d600EH2THC8ncxWEXEXZ1uH49Ian
bQKLBoqgcF6nQ0vEgWt+lzpVqluiLnAKN/akWbg2jzimKl1G8bCvL//b4q6Lr7e7
A0Fe9F5ppi+f2wp7ZEbaRa7hvIWMba2aI33TDFLgWBqed1eHL13A+HHqzqgfHt/+
XzX+dLoBAoGBAOCtmT5lJ5Hl0JwZnBd6gMSm0tMcReoZuYJHSs6HhZMBU5J6o21B
1TjRKdo4z+AzbWi+Vtx/Q9rW5d+16Rrr3mc0+i71o0aqUzVUU6yw0ublsJaL2J
kgW/mLtkU+3abDKaFdL0CkRg/CW9t/Elo1gQH8nLVVvPdMmiX5Q4NZCSAoGBAN2F
TNFjekrML0JqEyMnxhuBWH8itqTnlUhk7Kn9TVzW00sdNtsI5p3PiJv5sHWBtqiS
pm6x+E9mE24lKEIm5EdHDkqivZfGr4H0/RvraUJNeoLXs01yp7H1JoV0tuFza6y0
lG7F3JtZP6GMtu4ew+TumAWzTgURIAFJdKN0dczVAoGAerNz4FZ/8LbQYZ++ljep
wTuDHq3vJLud0Z87pGTwtuLfkDx3qgBtANWCBNJH/IpEiTzS73TmHhikcazs+bdx
onnaZNzIfyDklzu/UsqT+p01YvRVhkVuQMntFtHo4BoMQupRht60CN/qdHYS0Zib
h0lvAuTCSBv9D00nQ5wa7MkCgYAZCwXZMibUJ+s71eQd+FQkLeZEUtdWwzuU0Jys
xw8k7MAnpGDc0FBiD0FDy0GTFzWAKLwaDZKl30NZE2h0ujjaegT6mRVYAEU9KuYm
buGydjHgcU05YDnnG3DkZzaznCnTEzdiooCZiEUcWUI3H+G9RZlprGuTvZQTu6Z
u7gDLQKBgQCCCeGU+yKJ5dGcBdylMaVYGKuTE8sr/ccWTM9fJN8PDUDg4rYI8yHr
sjs7tlh/sPQHizC0euiW+07sHgHvzI9ClDyrbX4hgM3epdD8gs+5JDnNBEuxxMXc
XdT8BCTaMf7Qs4rzMqW7cZ2km70r00RfHUnoayRQsKc0XyEbShN7Zw==
-----END RSA PRIVATE KEY-----
```

Figura 2: Verificação da chave privada criada pela Cláudia.

David:

```
pc@pc-vivobook-asus-laptop-x507ma-f507ma:~/SegRedes$ openssl rsa -in privkey.pem -check
RSA key ok
writing RSA key
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAwkuEzf2z1tum2oxG+H6AK1mfgWwWwQZfcqbQ5hlQUj120+Jy
0hWETIXde5N3HM3vLFqk3HuyDhsZ38AoE0vQH0uJRoiuP2MI7nnttvcqxKL3edgV
edQJbAbOX+mGgWVvAYr1+LyrBrjkHLbjs3rmnaSJNveoYwR1KaSvfxwJw9bsEIHv
QfKktpvf7huTtYZjvQImBfPFQm9i14q5Q00x1rBbQAZVCYQ9EPenJx/aPMVhZTeI
X1+2gJxrqTqZm3lyTICIMh/GfKQZvpgNar7gzg8DDgmczkcZGvCYPowZdbPI1T2S
LyW+n4Q13opDm4imvLxVYUUCo9amf9pzBwJ/wIDAQABAoIBAQCnnnUdLSEmy2aA
JwLXQHMccev5ND6xlC4FurQGNcQs9V+9azoITIBr52yKPC0J6xCLxleWinUg4KSNC
SEmKlB4gFo43/pSs9Khw7FmrPkL0T0/HGycz6jySsQLCESDgVC8gfgZ3AkCvP6dRJ
/XI1lgK8v4TtGe14NxFI8t3AgBTgkNmImGxwr1oPH5A7eYbesESlweSXXa4XCN11
0psFbikm7gsetfLyTVtw2+r3ZJTfB6000PXssRRf3AdmaNCoQ0EVBaQNaAX0yggB
7UUYl5mfkecpmGqkEb3gznedhKDUIzjcywXXWbjBdGvJNjMCT11BPavjh1CC1cmS
uv8Ib/G5AoGBA04F22nqlyBmv1ntmejvNYpwwh6TqU2xdWY2wkddkXqM26bpdE3y
BE7kAgf630AMkgDTrU7BJXPKjCMBHzZ+8jRplNgVdCnctNedtZyFVZ0waRmjF+9v
9kabuXx8k2/pm+QZup5xD/ao73dcoiwgVCzW09S6tkLB3j1USZn0IPNVa0GBAND4
MD6uKWwBGxHMKrxKvJQRivjpL7k4rdzZ6AQ0ss28sBsK0LaCMCMkM30wdo6uSjZc
xPYkIS4d6nrJeetjqyw1XiBw/EWidFPKmjGm2wITNfmcbsc/1txCIg7yz+ftBsBF
Bv6wbTH81wnCw3lZMK8NaGVEp4GMTzQ1tj5iNHADAoGAbMkuhBuc50kukapfmq+h
t91bT2BLK9/UeVfzQWxhbJJsVbeBWX1QcYIST5VfV+NG46vbXNA4DuTZC7Kakmw8
572NssjzYKohWR6Sf6wM9cg980KysNNqKtFhkFbbh92sSy9bNMkV87U4ZURoNmS8
NBYNk0WZIZ+7tCo0zYYBV1UCgYBmc7gbkWHF7Qjbg1PS4wVvxrMRvCnksPazPjaN
kVS0n7Trn0hP0qblI80CDds1evrx11wazX3jAVHLn2oB6RysEQIZ/5D/hvVnh/K/
+yFW9B1vcczjCisL8/SExbD+5KxjqbQTPGZc4oc8Ytu5a+v9dyJeu/kv/515Xydg
kH9LBwKQC69uRts/KVU8o121MYBUakCgKMkMkccZtmDounCLTGeGHxRl0B1D1
B4FvChMddPXne0E1rk6a/U+/iCp4kAvo76zSDVrgeFMF3emTnufzWZunCJpINMt
ZQUhA0SpukMZQQ3e1r1nZyRIADhHGcantEhC+g97ljRcCmnGUXotg==
-----END RSA PRIVATE KEY-----
```

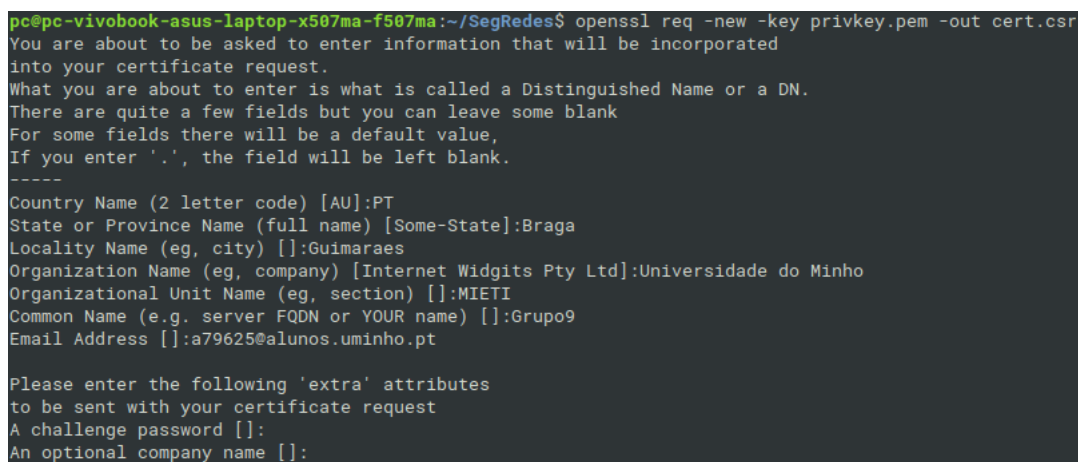
Figura 3: Verificação da chave privada criada pelo David.

Como se pode observar ambas as chaves privadas RSA estão em bom estado de funcionamento, pelo que poderão ser usadas para os fins de cifra e assinatura.

2.3. Gerar um pedido de certificado X.509

De modo a adquirir um certificado é necessário efetuar um pedido de certificado onde está incluído o par de chaves (privada e pública) assim como informação relevante que estará presente no certificado a criar.

- *openssl req -new -key privkey.pem -out cert.csr*



```
pc@pc-vivobook-asus-laptop-x507ma-f507ma:~/SegRedes$ openssl req -new -key privkey.pem -out cert.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:PT
State or Province Name (full name) [Some-State]:Braga
Locality Name (eg, city) []:Guimaraes
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Universidade do Minho
Organizational Unit Name (eg, section) []:MIETI
Common Name (e.g. server FQDN or YOUR name) []:Grupo9
Email Address []:a79625@alunos.uminho.pt

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

Figura 4: Efetua pedido de certificado.

Uma vez efetuado o pedido é possível verificar (Figura 5 e 6) se este foi efetuado corretamente e a informação que contém, através do comando apresentado de seguida.

- *openssl req -text -noout -verify -in cert.csr*

```

root@kali:~/certificados# openssl req -text -noout -verify -in cert.csr
verify OK
Certificate Request:
Data:
  Version: 1 (0x0)
  Subject: C = PT, ST = Braga, L = Guimaraes, O = Universidade do Minho, OU = MIETI, CN = Grupo9, emailAddress = a78232@alunos.uminho.pt
  Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public-Key: (2048 bit)
    Modulus:
      00:c2:6a:da:e6:c9:44:cf:1e:11:11:4b:fc:cc:27:
      de:b6:1b:c1:8e:b3:cc:ac:15:7e:0f:65:88:18:c6:
      b9:a4:74:15:6e:5e:be:dd:04:09:77:b0:32:49:6e:
      ae:ee:22:07:7b:9e:dd:5f:16:32:fe:50:6c:5d:1c:
      16:bc:ef:1e:d4:59:85:1d:49:e8:11:8a:b3:95:f8:
      4e:df:ac:ce:c0:e4:3f:5f:34:5d:61:51:96:7a:0d:
      40:1d:48:aa:c7:63:93:7b:15:68:4d:eb:bf:8e:e3:
      72:c3:cb:79:4c:7f:33:39:c0:1c:9d:62:3e:4d:2b:
      3c:09:d3:cf:4d:70:a0:7e:5b:de:58:f4:cf:ba:97:
      92:1f:63:09:fa:14:e2:e2:5d:ea:95:f1:28:16:91:
      f1:5d:40:2e:f4:91:2d:6d:a3:42:b3:0e:f7:10:ac:
      ec:92:e5:b7:15:8f:b2:e8:cc:5f:b7:e9:21:a6:8d:
      39:9c:d9:ed:8a:d8:ae:6a:c1:10:38:fd:d7:95:38:
      e7:67:72:ab:5f:bb:a0:22:fb:bb:d1:14:7b:e4:c7:
      80:e8:da:5d:4b:3b:d3:83:65:18:55:b5:c5:53:38:
      42:a4:fa:dd:11:33:67:c7:60:d0:55:c9:2e:5a:1c:
      fc:be:7e:e0:29:26:9d:ee:fd:0d:91:9f:7b:f6:71:
      d5:ed
    Exponent: 65537 (0x10001)
  Attributes:
    a0:00
  Signature Algorithm: sha256WithRSAEncryption
    bf:b1:b0:4d:fe:85:47:b5:79:98:f4:6f:85:d8:4e:8c:41:19:
    4f:ab:ce:78:aa:80:51:a8:31:d6:9d:f8:3c:8e:37:47:a7:2e:
    5a:92:7b:53:5e:91:30:fa:3d:a0:87:7e:51:bb:ae:b5:ae:51:
    1f:4c:31:61:06:f9:8d:2e:2f:0f:48:84:1f:7b:d2:96:36:5e:
    51:74:be:5b:05:5f:17:68:aa:af:1b:4e:6b:c0:93:da:cf:c8:
    0e:74:96:c6:77:c9:29:cb:73:57:ac:f7:88:d9:cf:4d:79:69:
    0a:59:05:57:6c:93:f9:e7:7f:5a:2f:4e:ea:06:3a:ef:67:2f:
    b6:e6:7a:d1:bb:11:b4:51:dc:8e:a0:b4:b0:30:f5:25:5c:21:
    50:f0:eb:61:43:c0:65:47:f2:58:fa:76:8b:98:73:7f:e8:9c:
    97:30:c8:df:bc:4a:9d:9d:67:71:1e:86:32:28:72:43:92:0b:
    e6:81:e9:1b:b2:ce:cf:de:a3:f4:ad:5a:2e:fc:2f:0a:01:db:
    2f:a5:d2:29:ca:0f:91:7a:05:13:13:b5:58:15:6b:bf:11:27:
    78:88:b5:21:8c:60:a7:9d:ee:a8:38:a6:aa:a6:d0:7e:1b:43:
    eb:86:c6:36:cc:86:ec:6d:94:2c:4c:24:13:84:a1:26:43:41:
    cf:23:82:cd

```

Figura 5: Verifica pedido de certificado da Cláudia.

```

pc@pc-vivobook-asus-laptop-x507ma-f507ma:~/SegRedes$ openssl req -text -noout -verify -in cert.csr
verify OK
Certificate Request:
Data:
  Version: 1 (0x0)
  Subject: C = PT, ST = Braga, L = Guimaraes, O = Universidade do Minho, OU = MIETI, CN = Grupo9, emailAddress = a79625@alunos.uminho.pt
  Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    Public-Key: (2048 bit)
    Modulus:
      00:c2:4b:84:cd:fd:b3:8a:db:a6:da:8c:46:f8:7e:
      80:2b:59:9f:83:05:b0:65:06:5f:72:a6:d0:e6:19:
      50:52:3d:76:d3:e2:72:3a:15:84:4c:8c:5d:7b:93:
      77:1c:cd:ef:2c:5a:a4:dc:7b:b2:0e:1b:19:df:c0:
      28:13:4b:d0:1d:4a:09:46:88:ae:3f:63:08:ee:79:
      ed:b6:f7:2a:c4:a2:f7:79:d8:15:79:d4:09:6c:06:
      ce:5f:e9:86:81:65:6f:01:8a:f5:f8:bc:ab:06:b8:
      e4:1c:b6:e3:b3:7a:e6:9d:a4:89:36:f7:a8:63:04:
      75:29:a4:af:7f:1c:09:c3:d6:ec:10:88:55:41:f2:
      a4:b6:9b:df:ee:1b:93:b5:86:63:bd:02:26:05:f3:
      c5:42:6f:62:d7:8a:b9:41:0d:31:d6:b0:5b:40:06:
      55:09:84:3d:d0:f7:a7:8f:1f:da:3c:c5:61:65:37:
      88:5f:5f:b6:80:9c:6b:a9:3a:99:9b:79:72:4c:80:
      88:32:1f:c6:7c:a4:19:be:98:0d:6a:be:e0:ce:0f:
      03:0e:09:9c:ce:47:19:1a:f0:98:3e:8c:19:75:b3:
      c8:d5:3d:92:2f:25:be:9f:84:22:de:8a:43:9b:88:
      a6:bc:bc:55:61:49:54:0a:8f:5a:99:ff:69:cc:1c:
      09:ff
    Exponent: 65537 (0x10001)
  Attributes:
    a0:00
  Signature Algorithm: sha256WithRSAEncryption
    5c:98:7d:1c:b9:d7:28:41:04:ee:c4:2e:9e:32:1a:55:53:11:
    75:7b:8d:28:fa:b8:90:47:84:79:c1:56:79:7e:2b:07:ea:3e:
    2f:ef:0a:7b:80:ea:53:40:58:05:a0:70:a5:b6:13:e4:7d:bb:
    2d:3c:62:bf:08:e5:4e:1e:04:1b:56:11:6f:2a:67:de:36:a1:
    b7:27:a5:0b:91:5b:dd:c9:61:86:e9:49:aa:44:6c:71:23:90:
    ab:27:11:d8:dd:b4:27:3c:3b:7b:a1:79:de:3b:65:bc:ac:f6:

```

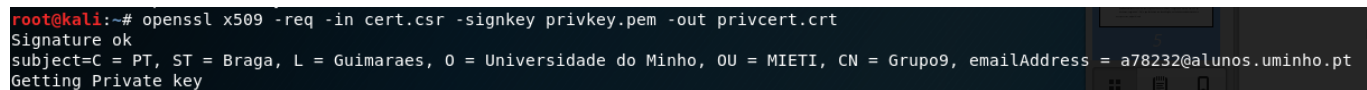
Figura 6: Verifica pedido de certificado do David.

2.4. Certificado auto-assinado

Através do comando ilustrado de seguida, cada elemento gera um certificado auto-assinado, isto é, assinado pela chave privada que criou anteriormente, não havendo uma CA de topo.

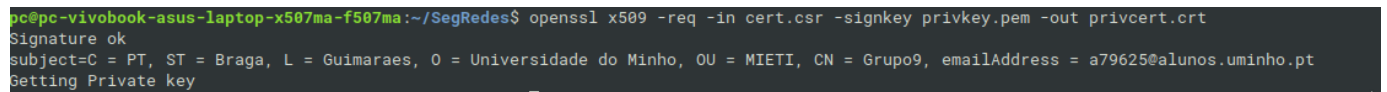
Para tal é usado o pedido de certificação que foi gerado previamente (*cert.csr*) e a chave privada (*privkey.pem*), resultando o certificado *privcert.crt*.

- `openssl x509 -req -in cert.csr -signkey privkey.pem -out privcert.crt`



```
root@kali:~# 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, OU = MIETI, CN = Grupo9, emailAddress = a78232@alunos.uminho.pt
Getting Private key
```

Figura 7: Criação de um certificado auto-assinado pela Cláudia.



```
pc@pc-vivobook-asus-laptop-x507ma-f507ma:~/SegRedes$ 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, OU = MIETI, CN = Grupo9, emailAddress = a79625@alunos.uminho.pt
Getting Private key
```

Figura 8: Criação de um certificado auto-assinado pelo David.

3. Servidor ADSS

3.1. Gerar par de chaves RSA

Para gerar o certificado da CA, primeiramente é necessário criar um par de chaves RSA (Figura 9).

The screenshot shows a 'New Service Key' dialog box. The title bar reads 'Key Manager > Service Keys > New'. The main area is titled 'Service Key'. It contains the following fields and options:

- Key Alias*:** A text box containing 'ETI-Grupo9'.
- Purpose*:** A dropdown menu with 'Certificate/CRL Signing' selected.
- Crypto Profile*:** A dropdown menu with 'Software' selected.
- Key Algorithm*:** A dropdown menu with 'RSA' selected.
- Key Length*:** A dropdown menu with '2048' selected.
- Description:** A large empty text area.
- ☐ **Allow the private key to be exported later as PFX/PKCS#12 file**

At the bottom right, there are 'OK' and 'Cancel' buttons.

Figura 9: Criação de um par de chaves.

3.2. Gerar certificado da Autoridade de Certificação

Uma vez criado o par de chaves já é possível criar o certificado da CA conforme representado na Figura 10, ao auto-assinar o certificado esta CA é considerada de topo.

The screenshot shows the 'Certificate Request Wizard' window. The 'General Details' section is at the top, showing 'Key Alias: ETI-Grupo9', 'Certificate Template: Default Certificate/CRL Signing Template', and 'Certificate Alias*: ETI-Grupo9-CA'. Below this is the 'Requested Certificate Details' section, which contains various fields for personal and organizational information. The 'Subject Alternative Name Details' section is below that, with checkboxes for 'rfc822Name', 'dNSName', 'IPAddress', and 'otherName'. The 'Certificate Processing Details' section is at the bottom, with radio buttons for 'Use Local CA (as configured in Manage CAs Module)', 'Use External CA', and 'Create Self-Signed Certificate' (which is selected). A 'Next' button is visible on the right side of the window.

General Details

Key Alias: ETI-Grupo9
Certificate Template: Default Certificate/CRL Signing Template [View Template]
Certificate Alias*: ETI-Grupo9-CA

Requested Certificate Details

Common Name*: ADSS Default
Given Name:
Surname:
Title:
Organization Unit: DSI
Organization: UMinho
Organization Identifier:
Email: a79625@alunos.uminho.pt
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:

☐ rfc822Name
☐ dNSName
☐ IPAddress
☐ otherName

Certificate Processing Details

☐ Use Local CA (as configured in Manage CAs Module)
☐ Use External CA
☒ Create Self-Signed Certificate

Figura 10: Criação do certificado auto-assinado da CA.

Na Figura 11 efetua-se a consulta do certificado da CA criado sendo possível observar a informação contido no mesmo.



Figura 11: Consulta do certificado da CA.

3.3. Gerar certificados assinados pela CA

Criação de um certificado para cada elemento do grupo, em resposta ao pedido (cert.csr), assinado pela CA.

Figura 12: Criação de um certificado para cada elemento do grupo.

Figura 13: Criação de um certificado para cada elemento do grupo.

Uma vez finalizada a criação dos certificados encontra-se ilustrado na Figura 14 a lista de certificados. É importante ressaltar que constam certificados para além dos referidos anteriormente dado que os elementos do grupo cometeram erros aquando do preenchimento da informação do pedido de certificado. De modo a não permitir o uso dos mesmos, estes foram revogados.

Showing page 1 of 1

Order by: Created At Descending Clear Search Search

	Certificate Alias	Valid From	Valid To	Source	Status
<input checked="" type="radio"/>	Claudia_novo	2019-03-28 17:09:34	2020-03-28 17:09:34	Manual Certification	Active
<input type="radio"/>	David_novo_certificado	2019-03-27 23:55:26	2020-03-27 23:55:26	Manual Certification	Active
<input type="radio"/>	Claudia	2019-03-21 18:16:32	2020-03-21 18:16:32	Manual Certification	Revoked
<input type="radio"/>	David	2019-03-21 18:12:09	2020-03-21 18:12:09	Manual Certification	Revoked

View Revoke Reinstall Delete Import Certificates

Figura 14: Lista de certificados assinados pela CA.

Após a criação dos certificados é possível a consulta dos mesmos (Figura 15 e 16).

Certificate Details

General Path

Version : 3

Serial No : 347c2b161efb3a179209c53d18b233ba60603604

Subject DN :

Email : a78232@alunos.uminho.pt
Common Name : Grupo9
Organisation Unit : MIETI
Organisation : Universidade do Minho
Locality : Gulmaraes
State : Braga
Country : PT

Issuer DN :

Common Name : ADSS Default
Organisation Unit : DSI
Organisation : UMinho
Email : a79625@alunos.uminho.pt
Country : PT

Signature Algorithm : sha256WithRSAEncryption

Validity :

From : 2019-03-28 17:09:34
To : 2020-03-28 17:09:34

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:C2:6A:DA:E6:C9:44:CF:1E:11:11:4B:FC:CC:27:DE:B6:1B:C1:8E:B3:CC:AC:15:
 :7E:0F:65:88:18:C6:B9:A4:74:15:6E:5E:BE:DD:04:09:77:B0:32:49:6E:AE:EE:22:07:7B:9E:
 DD:5F:16:32:FE:50:6C:5D:1C:16:BC:EF:1E:D4:59:85:1D:49:E8:11:8A:B3:95:F8:4E:DF:AC:
 CE:C0:E4:3F:5F:34:5D:61:51:96:7A:0D:40:1D:48:AA:C7:63:93:7B:15:68:4D:EB:BF:8E:E3:
 72:C3:CB:79:4C:7F:33:39:C0:1C:9D:62:3E:4D:2B:3C:09:D3:CF:4D:70:A0:7E:5B:DE:58:F4:
 CF:BA:97:92:1F:63:09:FA:14:E2:E2:5D:EA:95:F1:28:16:91:F1:5D:40:2E:F4:91:2D:6D:A3:4
 2:B3:0E:F7:10:AC:EC:92:E5:B7:15:8F:B2:E8:CC:5F:B7:E9:21:A6:8D:39:9C:D9:ED:8A:D8:
 AE:6A:C1:10:38:FD:D7:95:38:E7:67:72:AB:F5:BB:A0:22:FB:BB:D1:14:7B:E4:C7:80:E8:D
 A:5D:4B:3B:D3:83:65:18:55:B5:C5:53:38:42:A4:FA:DD:11:33:67:C7:60:D0:55:C9:2E:5A:1Q

Key Usage : nonRepudiation, keyEncipherment, digitalSignature

Extended Key Usage : emailProtection

Authority Key Identifier : DD:77:D3:E5:28:6A:1B:8A:C4:3E:CF:9A:82:E0:4D:73:A7:AF:7C:9

Subject Key Identifier : F3:3C:DB:F4:A8:F5:95:C4:77:DF:66:C8:6A:DF:64:1E:F1:A1:31:35 //

Thumbprint Algorithm : sha1

Thumbprint : lhjRkYNX4MApdFCxB8YzDA==

Figura 15: Consulta do certificado *Claudia_novo*.



Figura 16: Consulta do certificado *David_novo_certificado*.

3.4. Gerar Certificados PKCS12

Para ser possível assinar e encriptar mensagens em diversas aplicações torna-se necessário possuir um ficheiro no formato PKCS12 assim, recorrendo ao comando exibido de seguida, criámos o ficheiro utilizando o certificado público assinado pela nossa CA, a chave privada e o certificado da CA.

- `openssl pkcs12 -export -in pubcert.pem -inkey privkey.pem -certfile CAcert.pem -name "my-name" -out priv-pkcs12.p12`

```
root@kali:~/certificados/Prints# openssl pkcs12 -export -in Claudia_novo.pem -inkey privkey.pem
-certfile CAcert.pem -name "Claudia" -out claudia_novo-pkcs12.p12
Enter Export Password:
Verifying - Enter Export Password:
```

Figura 17: Criação do ficheiro no formato PKCS12(Cláudia).

```
pc@pc-vivobook-asus-laptop-x507ma-f507ma:~/SegRedes$ openssl pkcs12 -export -in David_novo_certificado.pem -inkey privkey.pem -certfile CA
id.p12
Enter Export Password:
Verifying - Enter Export Password:
```

Figura 18: Criação do ficheiro no formato PKCS12(David).

3.5. Instalação dos certificados

De modo a utilizar os certificados em diversas aplicações é necessário instalar os mesmos no Sistema Operativo (Figura 19 e 20), caso o pretendido seja assinar mensagens de correio eletrónico também é requerido instalar os certificados no cliente de *e-mail* (Figura 21).

Na figura seguinte é possível verificar que o certificado da CA localiza-se nos certificados de raiz, uma vez que é responsável pela emissão dos certificados públicos que cada elemento irá utilizar para assinar e encriptar mensagens.

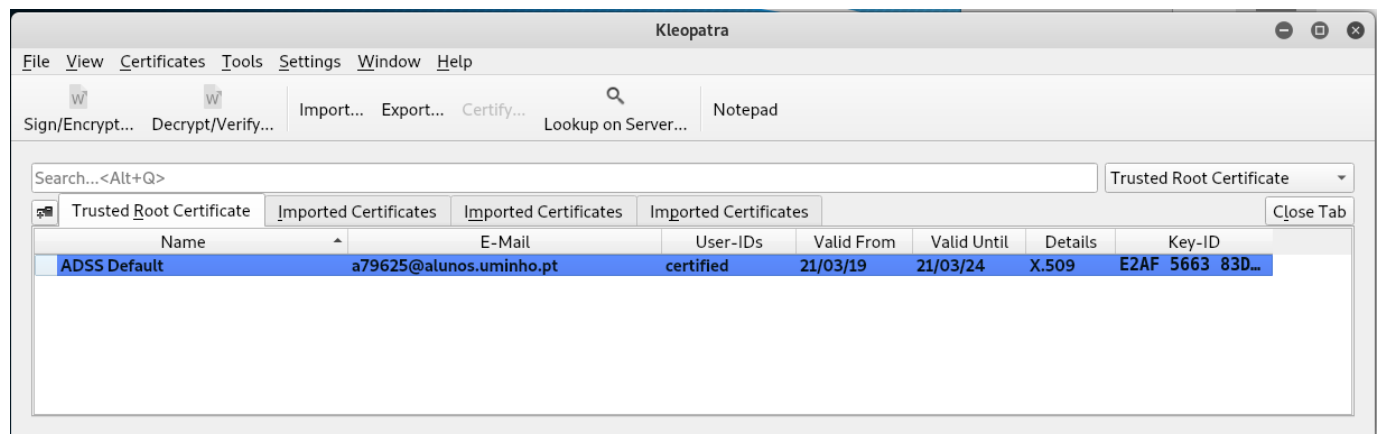


Figura 19: Definição do certificado da CA como certificado de raiz.

Os certificados públicos de cada elemento encontram-se nos certificados de confiança de modo a ser possível assinar/cifrar assim como verificar assinaturas/decifrar.

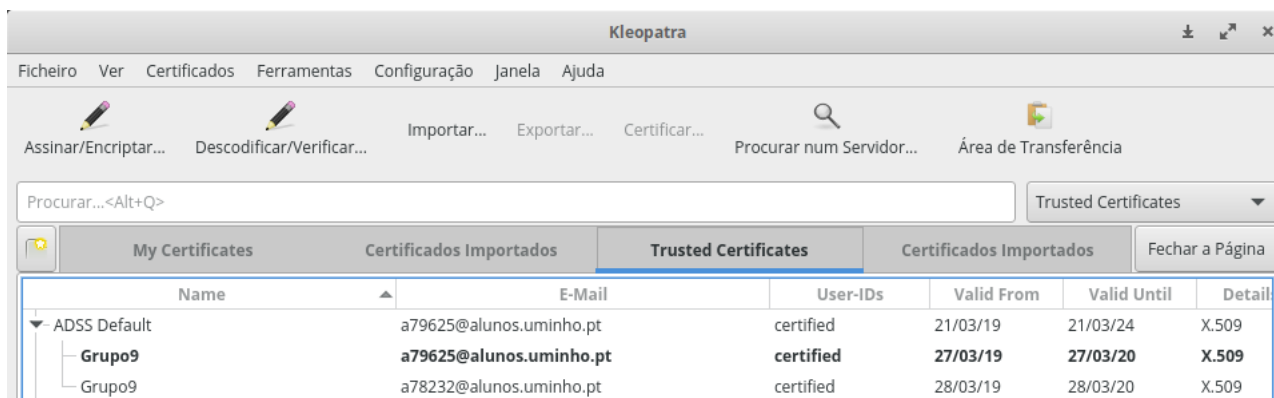


Figura 20: Definição dos certificados de cada elemento como certificados de confiança.

Na figura seguinte efetua-se a configuração do cliente de *e-mail Thunderbird*, adicionando em "Autoridades" o certificado da CA e em "Os seus certificados" o certificado público associado ao endereço eletrónico .

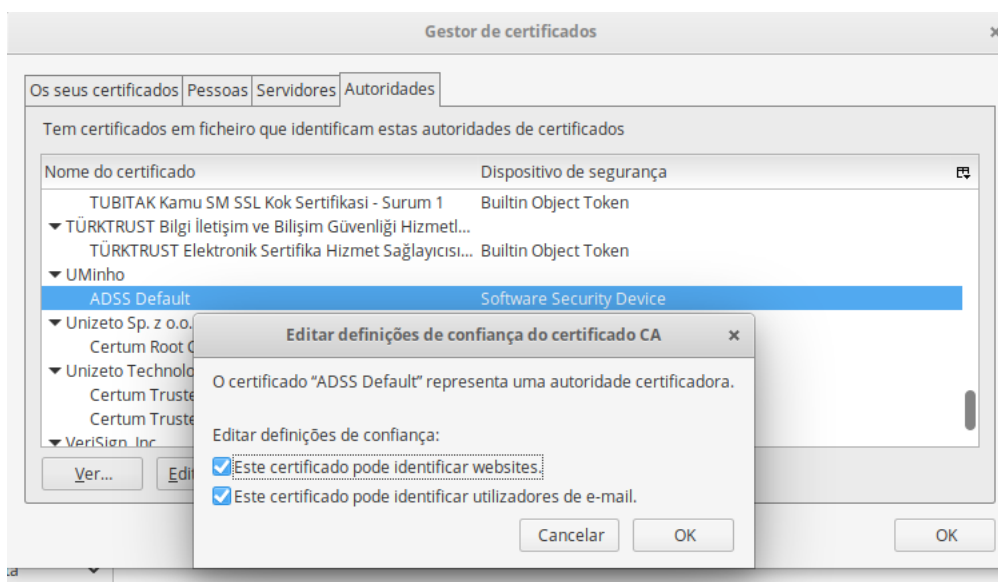


Figura 21: Configuração do cliente de *e-mail Thunderbird*.

3.6. Assinar digitalmente documento

Adicionalmente, o grupo decidiu assinar um documento através do "Adobe Acrobat Reader", sendo observável na Figura 22 a validação da assinatura.



Figura 22: Assinatura de um documento.

4. Troca segura de mensagens

De seguida procedemos ao envio de mensagens, de forma segura, usando para isso o cliente de e-mail ThunderBird, o gestor de certificados Kleopatra, os certificados X.509 (gerados anteriormente no OpenSSL) e certificados PGP (gerados com recurso a um *plug-in* do ThunderBird, o Enigmail).

4.1. Troca de mensagens usando certificados X.509

Nesta troca de mensagens foi demonstrado os princípios do funcionamento do protocolo S/MIME, no qual, numa fase inicial existe uma troca de certificados (extraíndo-se as chaves públicas), e depois ambos os intervenientes podem trocar mensagens encriptadas entre si.

Inicialmente um elemento do grupo (David, neste exemplo), envia uma mensagem apenas digitalmente assinada, tal como mostra a Figura 23.

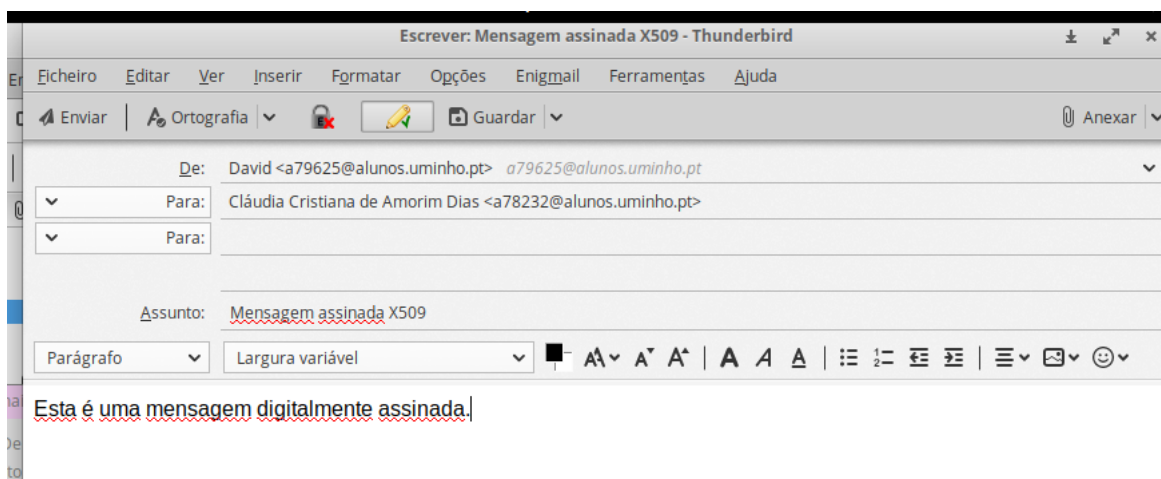


Figura 23: Envio de uma mensagem assinada.

Após isto, poderá verificar-se como mostra na Figura 24, que o outro elemento do grupo (Cláudia, neste exemplo) recebeu uma mensagem assinada, com uma assinatura que é válida, uma vez que ambos elementos do grupo adicionaram às entidade de confiança do seu sistema operativo e do cliente de *e-mail*, a autoridade de certificação de ambos os certificados.

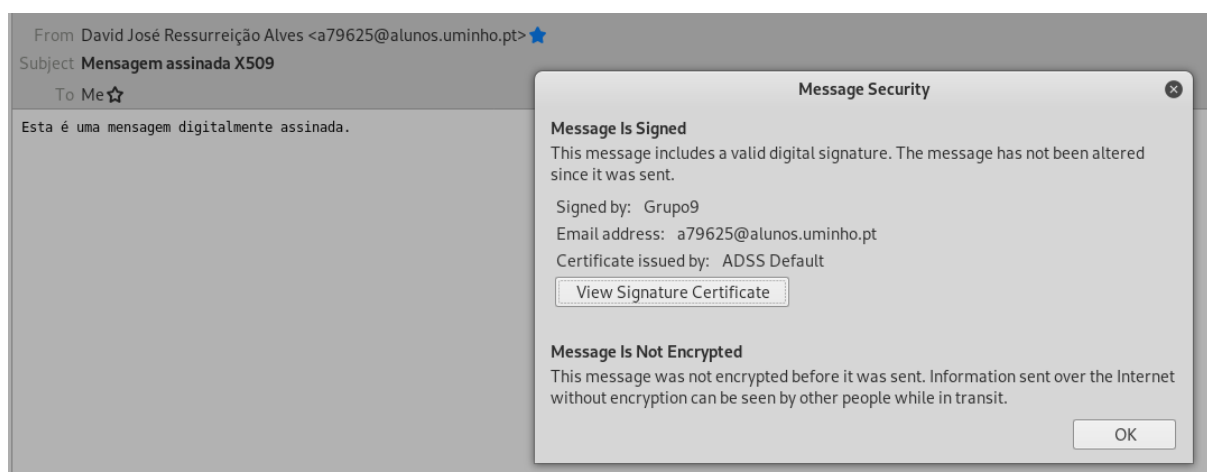


Figura 24: Receção da mensagem assinada.

Com a receção desta mensagem, a Cláudia tem agora a chave pública do David, e poderá enviar-lhe mensagens encriptadas. Mas antes a Cláudia envia para o David uma mensagem apenas assinada por ela, como mostra a figura 25. Assim, o David poderá ter acesso à chave pública da Cláudia e poderão ambos trocar mensagens entre si, de forma encriptada.

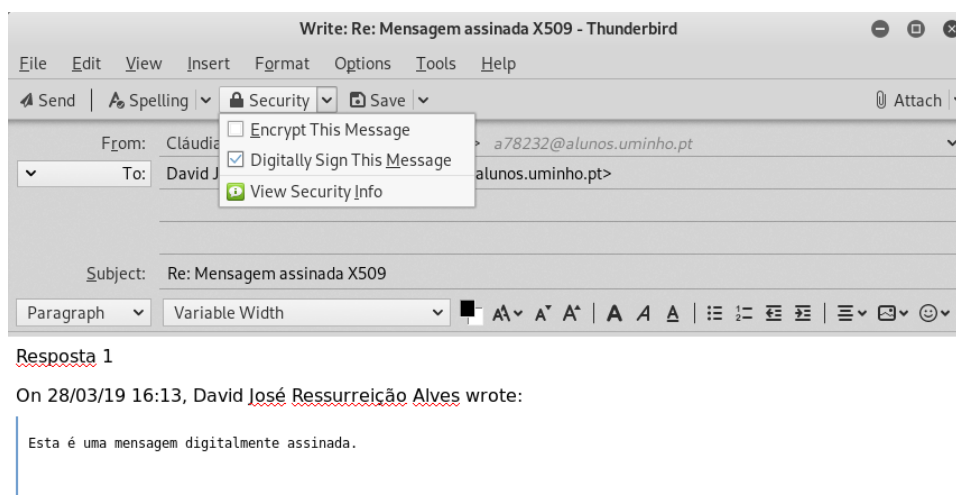


Figura 25: Resposta assinada à mensagem anterior.

De seguida, o David envia para a Cláudia uma mensagem assinada e encriptada (usando a chave pública da Cláudia), e a Cláudia como mostra a figura 26, recebe a mensagem encriptada que descripta usando a sua chave privada associada à chave pública com que o David encriptou a mensagem.

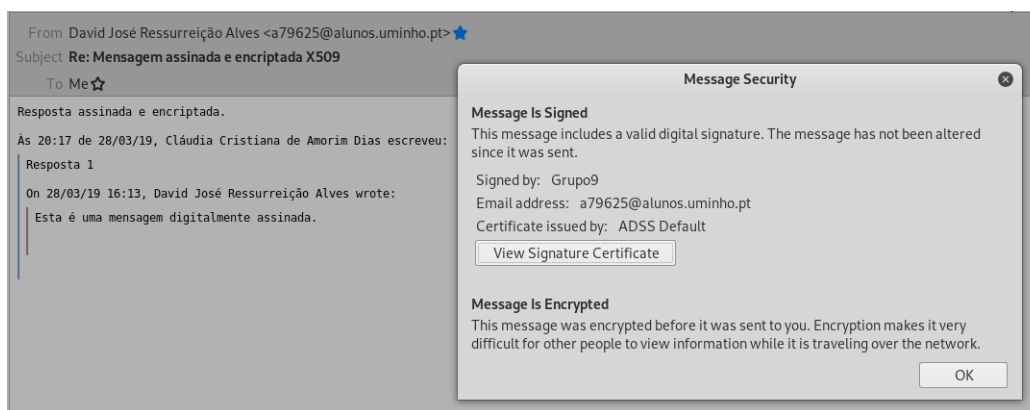


Figura 26: Receção de uma mensagem assinada e encriptada.

De seguida, a Cláudia envia para o David, também uma mensagem encriptada com a chave pública do David, e o David descripta com a chave privada a mensagem que recebe e verifica o conteúdo da mesma, e que esta foi assinada pela Cláudia, como se vê na seguinte figura.

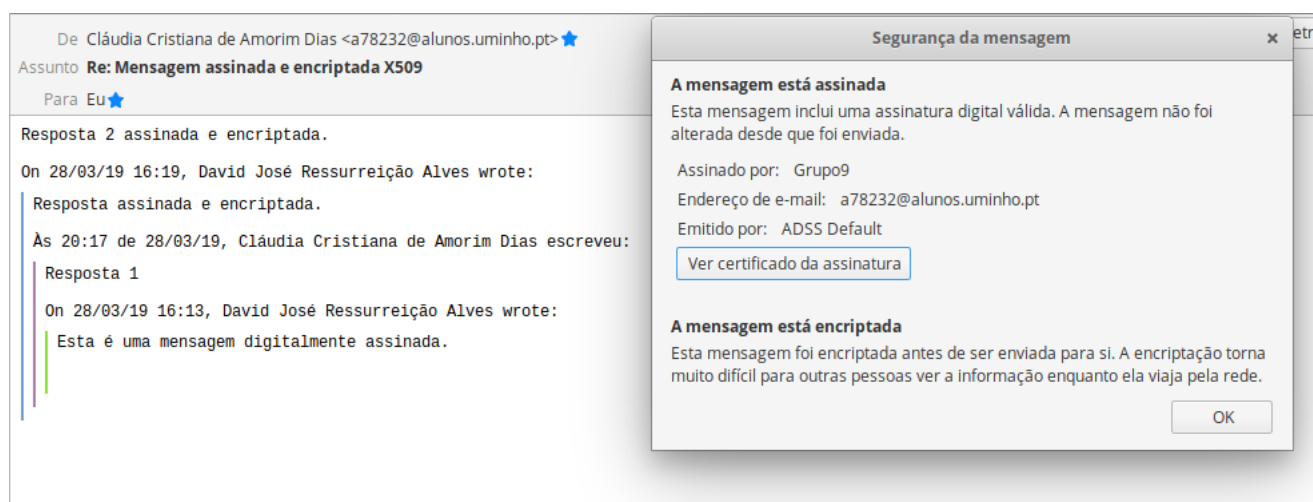


Figura 27: Receção da mensagem encriptada e assinada.

4.2. Troca de mensagens usando certificados PGP

Recorrendo à ferramenta *Enigmail*, que permite gerar chaves PGP, foi efetuada a troca de mensagens entre os elementos. Na Figura 28 são apresentadas as chaves que cada elemento tem de possuir no seu cliente de *e-mail*.

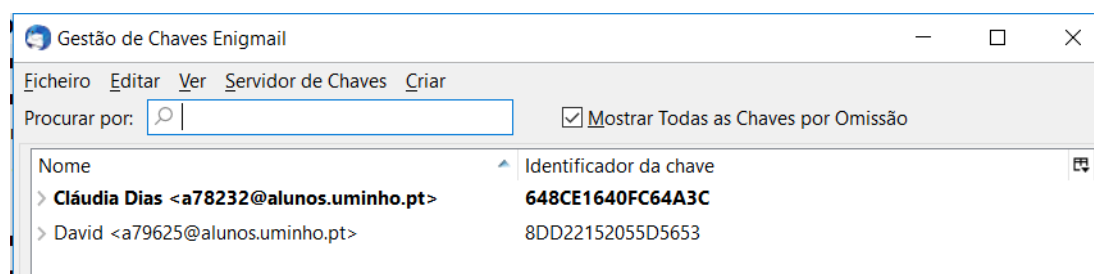


Figura 28: Lista de chaves PGP.

Inicialmente envia-se uma mensagem que é assinada com a chave privada PGP e cifrada com a chave pública do destinatário (Figura 29).

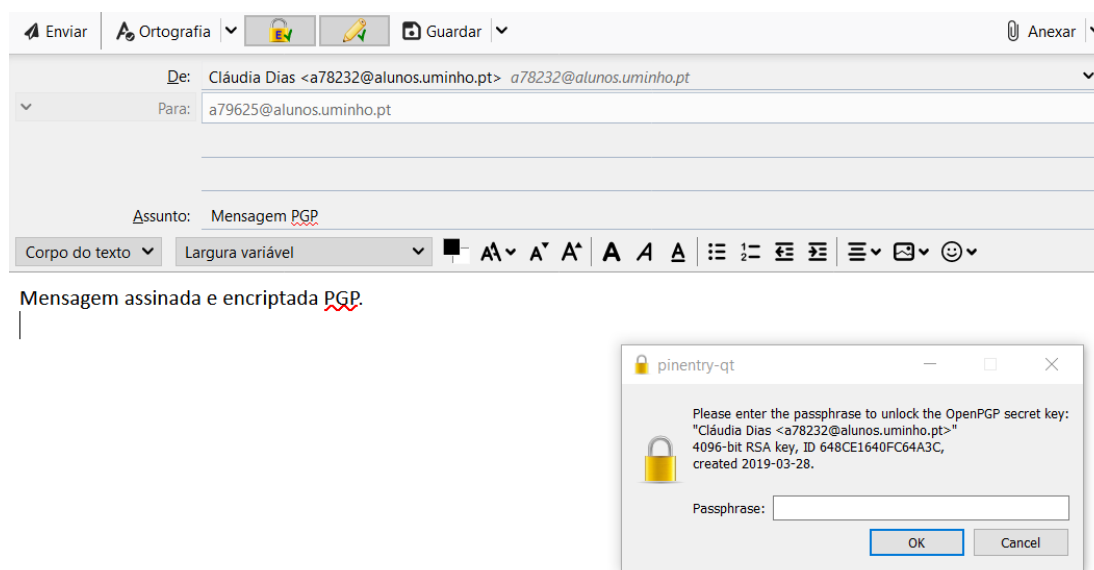


Figura 29: Envio de mensagem assinada e encriptada.

Aquando a receção da mensagem (Figura 30) esta encontra-se cifrada e apenas é decifrada se o receptor inserir a *passphrase* da sua chave privada.

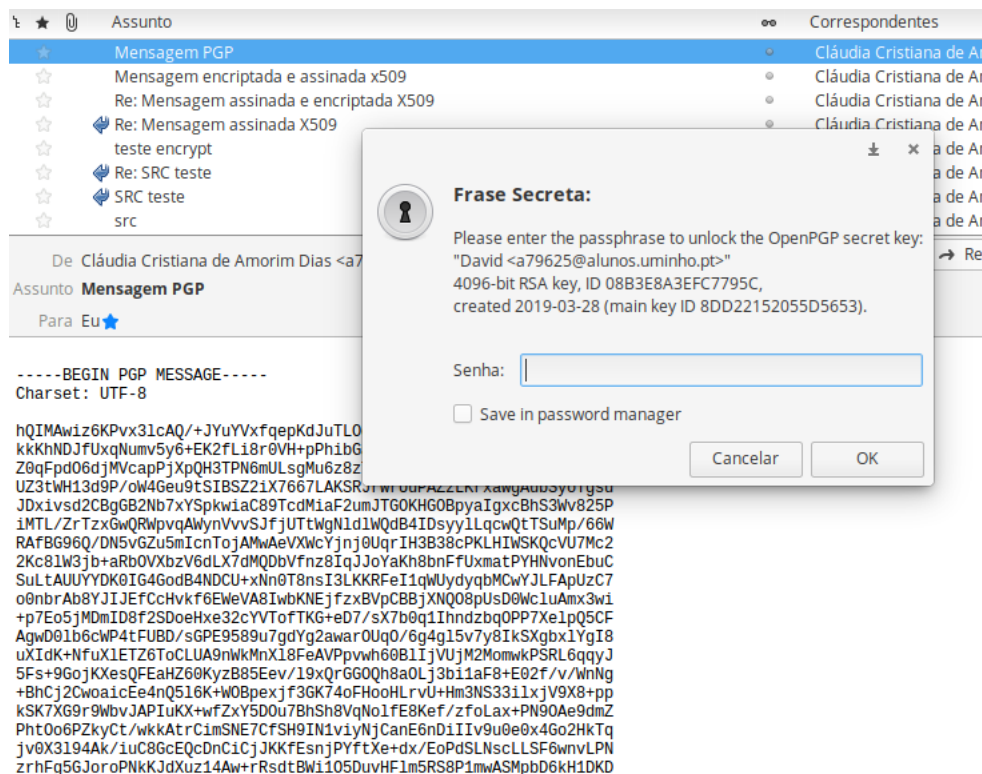


Figura 30: Impossibilidade de decifrar.

Na Figura 31, após a inserção da *passphrase* a mensagem recebida é decifrada sendo também apresentada a assinatura da mesma.

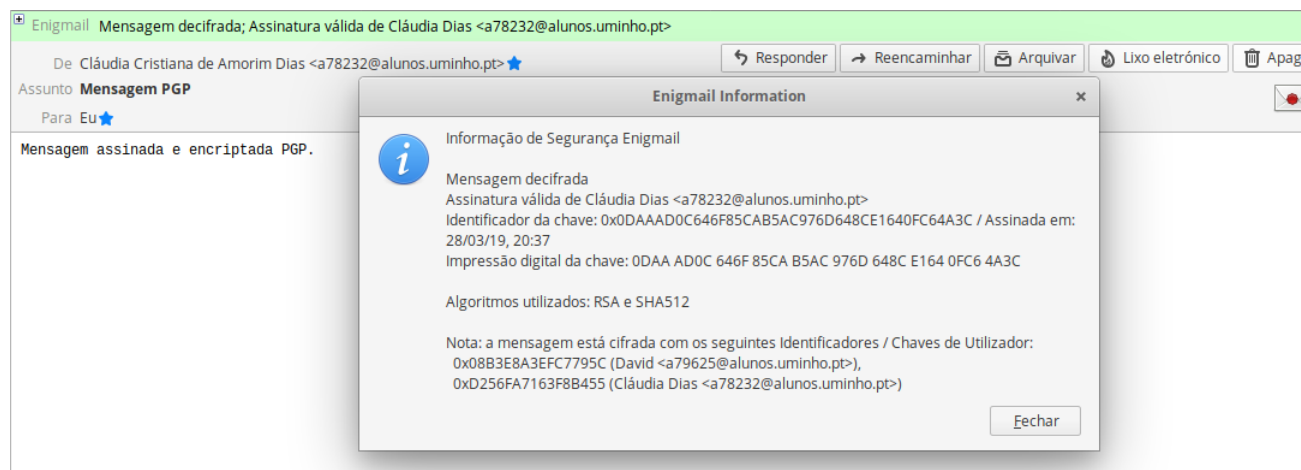


Figura 31: Decifra e verifica assinatura.

4.3. Troca de mensagens entre grupos

Tal como pretendido, efectuámos também comunicações com outros grupos de forma a comprovar o bom funcionamento das nossas CA's.

O grupo com o qual fizemos a trocas de mensagens assinada e encriptadas foi o grupo 8.

Na seguinte figura podemos observar que o grupo 8 após ter instala o certificado público da Cláudia e do David, e o certificado da nossa CA, puderam descriptar a mensagem por nós enviada e verificar a assinatura da Cláudia.

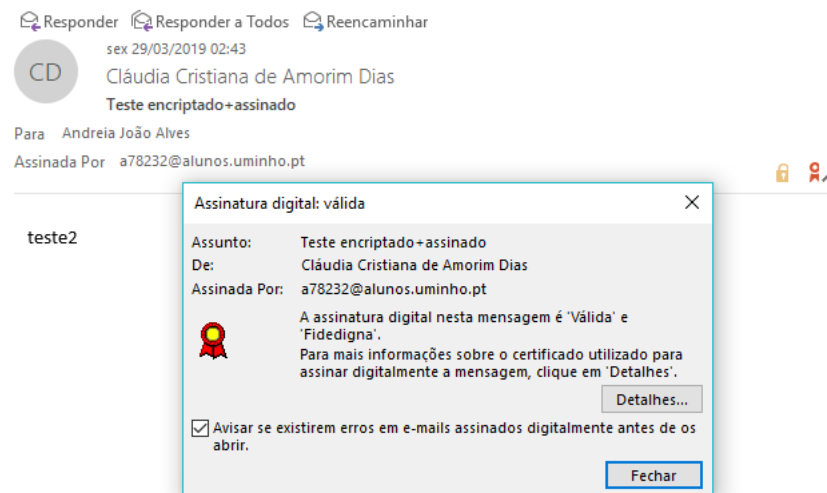


Figura 32: Verificação da assinatura.

Finalmente, depois de termos instalado os certificados públicos de cada elemento do grupo 8 e da sua CA, descriptámos uma mensagem enviada por esse grupo e verificámos a sua respetiva assinatura, como mostra a seguinte figura.

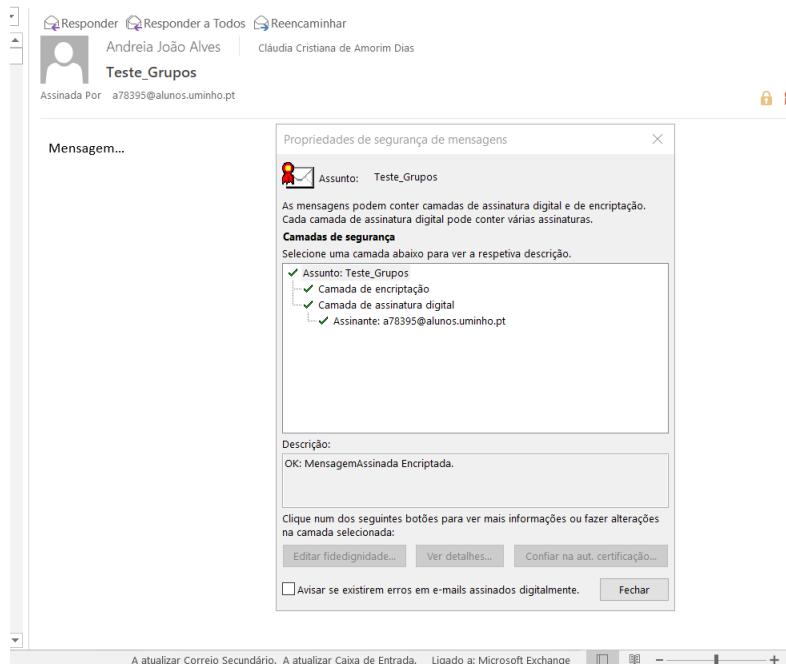


Figura 33: Receção da mensagem encriptada e assinada pelo Grupo 8.