

**Universidade do Minho**  
Escola de Engenharia

## CIBERSEGURANÇA

# TP3 - CHAVES DE CIFRA, CERTIFICADOS E O PGP

Autores:

Inês Barreira Marques - a84913@alunos.uminho.pt

José Carlos Peixoto Ferreira - a85497@alunos.uminho.pt

Marcos Alexandre Ferreira Martins - a84481@alunos.uminho.pt

Rui Filipe Ribeiro Freitas - pg47639@alunos.uminho.pt

Tiago João Pereira Ferreira - pg47692@alunos.uminho.pt

7 de abril de 2022

# Índice

<b>1</b>	<b>Gestão de chaves</b>	<b>4</b>
1.1	Opção PGP . . . . .	4
1.2	Opção X509 . . . . .	11
<b>2</b>	<b>Enviar e receber mensagens seguras</b>	<b>19</b>
2.1	Opção PGP . . . . .	19
2.2	Opção X509 . . . . .	26
<b>3</b>	<b>Proteger documentos locais</b>	<b>31</b>
<b>4</b>	<b>Conclusão</b>	<b>33</b>

## Lista de Figuras

1	Ambiente Kleopatra. . . . .	4
2	Criação da chave no Kleopatra. . . . .	4
3	Configuração Avançada da chave. . . . .	5
4	Detalhes do Certificado. . . . .	6
5	Chave master e subchave. . . . .	6
6	Configuração do servidor. . . . .	7
7	Exportação para o servidor. . . . .	7
8	Confirmação da exportação do Certificado no Kleopatra. . . . .	8
9	Confirmação da exportação do Certificado no servidor. . . . .	8
10	Pesquisa por e-mail. . . . .	8
11	Pesquisa por nome. . . . .	9
12	Certificação da chave pública. . . . .	9
13	Confirmação da Certificação. . . . .	10
14	Criação do par de chaves. . . . .	11
15	Verificação do estado da chave privada. . . . .	11
16	Criação do pedido de certificado. . . . .	12
17	Verificação do estado do pedido de certificado. . . . .	12
18	Criação do certificado auto assinado. . . . .	13
19	Verificação do estado do certificado auto assinado. . . . .	13
20	Criação do repositório e CA <i>root</i> . . . . .	14
21	Criação das bases de dados e realizado um CA <i>request</i> . . . . .	14
22	Criação de um certificado CA auto assinado. . . . .	15
23	Criação das diretorias, bases de dados e de um CA <i>request</i> . . . . .	15
24	Criação do certificado CA assinado pela <i>root</i> CA. . . . .	16
25	Realização do email <i>request</i> . . . . .	16
26	Criação do certificado email. . . . .	17
27	Criação do ficheiro no formato PKCS12. . . . .	17
28	Verificação do ficheiro no formato PKCS12 (1). . . . .	18
29	Verificação do ficheiro no formato PKCS12 (2). . . . .	18
30	Inserir chaves públicas e privadas no Thunderbird. . . . .	19
31	Importação da chave privada e pública do José. . . . .	20
32	Importação da chave privada e pública do Tiago. . . . .	20
33	Importação da chave pública do Tiago no Thunderbird do José. . . . .	21

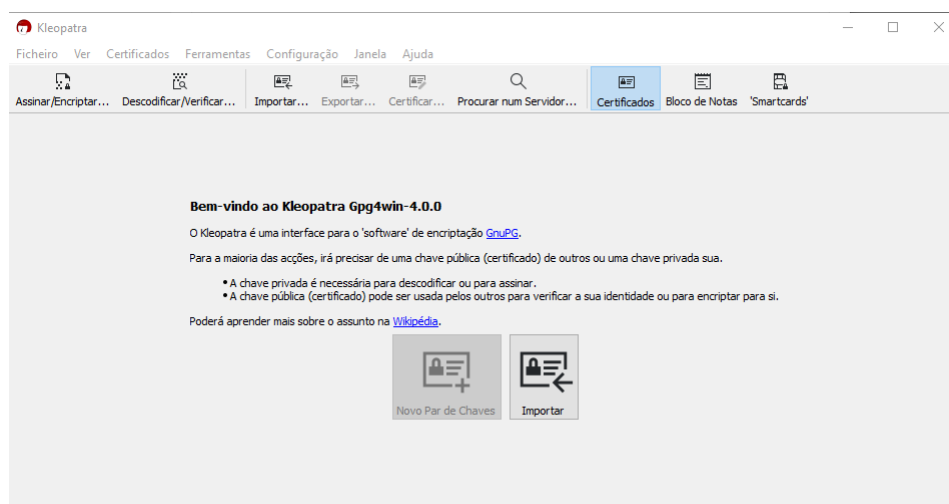
34	Importação da chave pública do José no Thunderbird do Tiago. . . . .	21
35	Exemplo de Envio de uma mensagem PGP. . . . .	22
36	Receção da mensagem do José. . . . .	22
37	Receção da mensagem do Tiago. . . . .	23
38	Revogação no Kleopatra. . . . .	23
39	Geração do Certificado de Revogação. . . . .	24
40	Confirmação da geração do certificado. . . . .	24
41	Certificado de Revogação. . . . .	24
42	Chave Revogada no Thunderbird. . . . .	25
43	Tentativa de envio de um e-mail após revogação. . . . .	25
44	Importação do certificado da CA. . . . .	26
45	Verificação do certificado da CA. . . . .	26
46	Verificação do certificado do utilizador. . . . .	27
47	Configuração da assinatura digital. . . . .	28
48	Envio de um e-mail do Rui para o Marcos e Inês. . . . .	28
49	Receção dos e-mails do Marcos e da Inês. . . . .	29
50	Revogação do certificado do Rui. . . . .	29
51	Comprovativo da revogação do certificado. . . . .	30
52	Opção para assinar/cifrar a pasta. . . . .	31
53	Escolha do certificado e pasta. . . . .	31
54	Opção para decifrar a pasta. . . . .	32

# 1 Gestão de chaves

## 1.1 Opção PGP

- **Passo 1:**

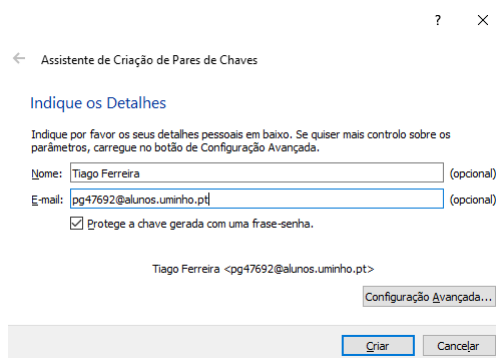
De forma a gerar um certificado PGP, foi instalado o gestor de certificados Kleopatra no ambiente do Windows.



**Figura 1:** Ambiente Kleopatra.

- **Passo 2:**

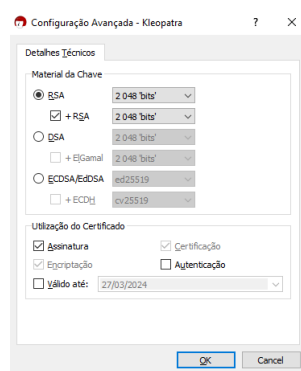
É possível observar a criação de uma nova chave PGP, onde é atribuído um nome e email à mesma.



**Figura 2:** Criação da chave no Kleopatra.

- **Passo 3:**

Usando a opção Advanced pode escolher-se o algoritmo de geração de chaves. Foi escolhido o algoritmo RSA 2048 bits. O algoritmo RSA é um algoritmo assimétrico, uma vez que dispõe de duas chaves, uma pública e uma privada. Este é usado em aplicações online, como por exemplo em trocas de e-mails. As mensagens são cifradas com a chave pública e só podem ser decifradas com a respetiva chave privada. Foi também desabilitada a data limite de validade.



**Figura 3:** Configuração Avançada da chave.

- **Passo 4:**

A Passphrase utilizada foi grupo2ciber.

- **Passo 5:**

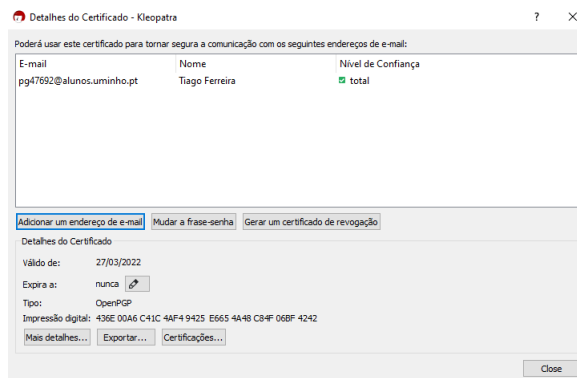
É dada a possibilidade da publicação da chave pública, não sendo esta publicação obrigatória ou necessária.

- **Passo 6:**

Os atributos mais relevantes da assinatura e das chaves identificados pelo grupo são:

- Data de criação: 27/03/2022
- Validade: Nunca
- Tipo de chave: OpenPGP
- Impressão digital: 436E 00A6 C41C 4AF4 9425 E665 4A48 C84F 06BF 4242

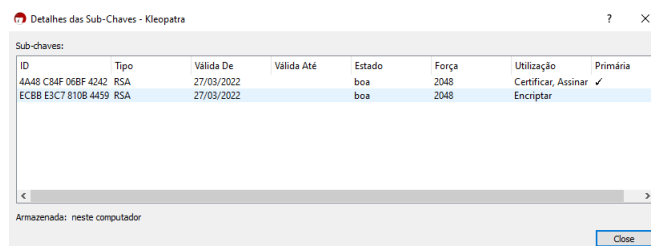
A chave apresentada na figura abaixo representa a chave pública, sendo ela o elemento que relaciona a assinatura com a nossa chave privada. Para a geração da assinatura digital esta é assinada com a chave privada sendo posteriormente verificada com a chave pública.



**Figura 4:** Detalhes do Certificado.

- **Passo 7:**

Na figura 5 pode ver-se a nossa chave master, usada para certificar e assinar, e uma subchave, usada para cifrar informação. Tanto a chave master como a subchave possuem parte pública e parte privada. Na chave master, a parte privada é utilizada para assinar/certificar já a parte pública é usada para a validar a assinatura gerada. Na subchave, a parte pública é utilizada para cifrar os dados da qual a respetiva parte privada serve para decifrar. Existe a necessidade de manter a chave master em segredo, e por isso são geradas as subchaves, que são assinadas pela chave master. Esta assinatura faz com que quando as subchaves são expostas não são gerados problemas maiores, uma vez que estas podem ser revogadas pela master, preservando a confidencialidade da chave master.

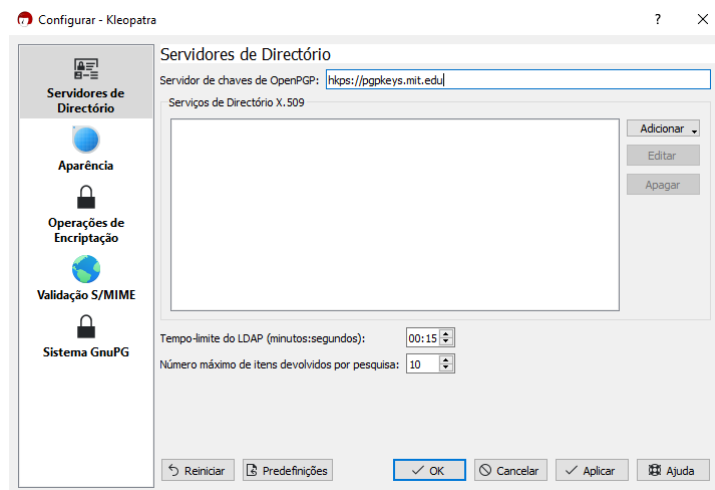


**Figura 5:** Chave master e subchave.

- **Passo 8:** Para obter um certificado do tipo X509 usando o par de chaves criado anteriormente apenas seria necessário fazer um pedido a uma CA (Certification Authority).

- **Passo 9:**

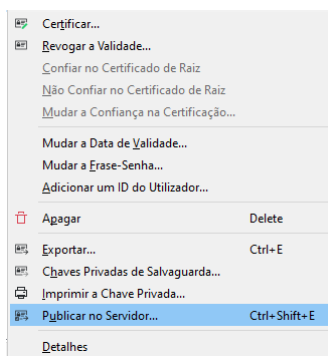
Na figura 6 podemos verificar a configuração do servidor `http://pgpkeys.mit.edu` que é usado para exportar a nossa chave pública.



**Figura 6:** Configuração do servidor.

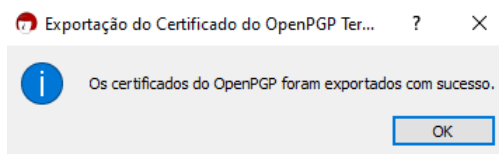
- **Passo 10:**

Neste passo é feita a exportação para o servidor como exemplificado na Figura 9 e depois a confirmação no servidor e no Kleopatra como se pode ver nas figuras seguintes.



**Figura 7:** Exportação para o servidor.





**Figura 8:** Confirmação da exportação do Certificado no Kleopatra.

Type	bits/keyID	Date	User ID
pub	2048R/ <a href="#">068F4242</a>	2022-03-27	<a href="#">Tiago Ferreira &lt;pg47692@alunos.uminho.pt&gt;</a>

**Figura 9:** Confirmação da exportação do Certificado no servidor.

Consultando o servidor `http://pgpkeys.mit.edu` e usando o e-mail e nome, é possível realizar uma pesquisa das chaves públicas existentes no servidor como demonstrado nas figuras 10 e 11.

### Search results for 'uminho pt hsantos dsi'

Type	bits/keyID	Date	User ID
pub	2048R/ <a href="#">18A842EA</a>	2018-11-01	<a href="#">Henrique M D Santos &lt;henrique.dinis.santos@gmail.com&gt;</a> HSantos <henrique.dinis.santos@dsi.uminho.pt> Henrique Santos <henrique.dinis.santos@gmail.com>
pub	2048R/ <a href="#">3473AE1C</a>	2016-09-14	<a href="#">Henrique Santos (Chave para uso na UH) &lt;hsantos@dsi.uminho.pt&gt;</a>
pub	1024D/ <a href="#">475D4617</a>	2006-07-13	<a href="#">Henrique M D Santos (Ho) &lt;hsantos@dsi.uminho.pt&gt;</a>
pub	1024D/ <a href="#">3AE27210</a>	2003-11-14	*** KEY REVOKED *** [not verified] <a href="#">Henrique M D Santos &lt;hsantos@dsi.uminho.pt&gt;</a> Henrique M D Santos (Para uso pessoal) <henrique.dinis.santos@gmail.com> [user attribute packet]
pub	1024D/ <a href="#">319D3084</a>	2001-06-15	<a href="#">Henrique Manuel Dinis dos Santos &lt;hsantos@dsi.uminho.pt&gt;</a>

**Figura 10:** Pesquisa por e-mail.

### Search results for 'santos henrique'

Type	bits/keyID	Date	User ID
pub	3072R/49EEF789	2022-02-24	<a href="#">Paulo Henrique dos Santos &lt;ounnerbr@gmail.com&gt;</a>
pub	3072R/26B2A788	2021-05-19	<a href="#">Henrique Santos &lt;hfigueiredosantos@tecnico.ulisboa.pt&gt;</a>
pub	3072R/50A4FFEF	2021-05-17	<a href="#">alexandre henrique santos grisende &lt;alexandre.grisende@aedb.br&gt;</a>
pub	3072R/D8EAD5D7	2021-05-17	<a href="#">alexandre henrique santos grisende &lt;alexandre.grisende@aedb.br&gt;</a>
pub	2048R/EC68DA08	2020-04-23	<a href="#">joao.h.santos@layer8.pt</a> João Henrique Santos <joao.h.santos@layer8.pt>
pub	2048R/5E4588DA	2020-02-18	<a href="#">JORGE HENRIQUE SANTOS GARCEZ &lt;mistergarcez@hotmail.com&gt;</a>
pub	2048R/18A842EA	2018-11-01	<a href="#">Henrique M D Santos &lt;henrique.dinis.santos@gmail.com&gt;</a> HSantos <henrique.dinis.santos@dsi.uminho.pt> Henrique Santos <henrique.dinis.santos@gmail.com>
pub	2048R/86F90D28	2018-10-23	<a href="#">Henrique Santos &lt;henrique.santos@inf.aedb.br&gt;</a>
pub	3072R/F3C5E85D	2018-08-29	<a href="#">Henrique dos Santos Goulart &lt;henrique.goulart@chaordicsystems.com&gt;</a>

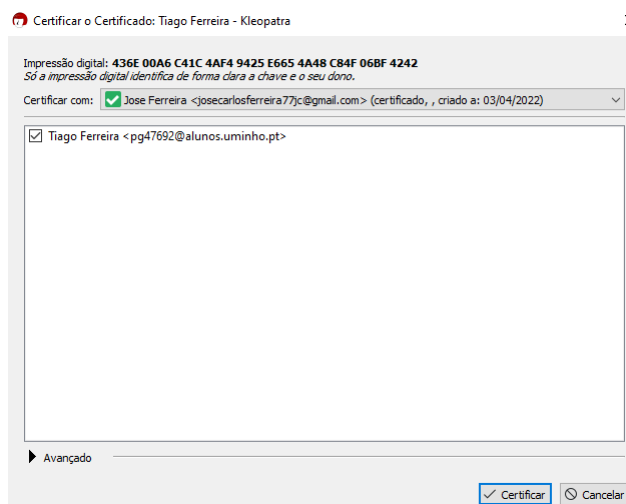
**Figura 11:** Pesquisa por nome.

Efetuando a pesquisa com nome pode ver-se que são apresentados mais resultados, isto porque o nome é um atributo comum a vários utilizadores, enquanto que o e-mail é único para cada utilizador, daí aparecem menos resultados.

- **Passo 11:**

Utilizando o Gmail foi enviada a chave pública após a exportação da mesma no Kleopatra para um formato .txt para o endereço e-mail do colega.

Após a receção e o download da chave pública procedeu-se à certificação da mesma, exemplificado na figura 12.



**Figura 12:** Certificação da chave pública.

Após a certificação pode ver-se no Kleopatra a confirmação da certificação, figura 13.

Nome	E-mail	ID's do Utilizador	Válida De	Válida Até	ID da Chave
Tiago Ferreira	pg47692@alunos.uminho.pt	certificado	27/03/2022		4A48 C84F 06BF 4242

**Figura 13:** Confirmação da Certificação.

- **Passo 12:**

Após a realização destes passos os colegas estão prontos a enviar mensagens seguras entre eles.

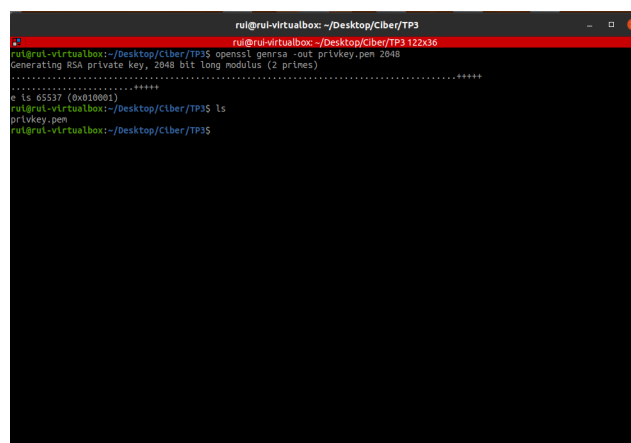
## 1.2 Opção X509

- **Passo 13:**

Para o desenvolvimento da opção X509 foi utilizada uma distribuição *Ubuntu* que já possui a biblioteca OpenSSL instalada.

- **Passo 14:**

Foi gerado um par de chaves RSA executando o comando apresentado na figura seguinte.



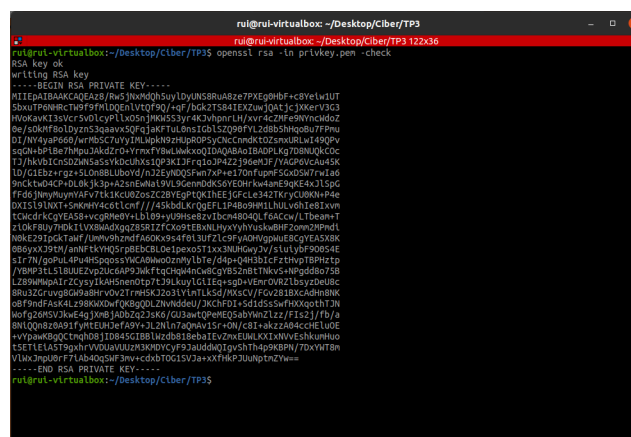
```

rul@rul-virtualbox: ~/Desktop/Ciber/TP3
rul@rul-virtualbox:~/Desktop/Ciber/TP3$ openssl genrsa -out privkey.pem 2048
Generating RSA private key, 2048 bit long modulus (2 primes)
.....+++++
e 65537 (0x10001)
rul@rul-virtualbox:~/Desktop/Ciber/TP3$ ls
privkey.pem
rul@rul-virtualbox:~/Desktop/Ciber/TP3$

```

**Figura 14:** Criação do par de chaves.

Após a criação do par de chaves, foi aberto o ficheiro para verificar a chave privada com o comando apresentado de seguida.



```

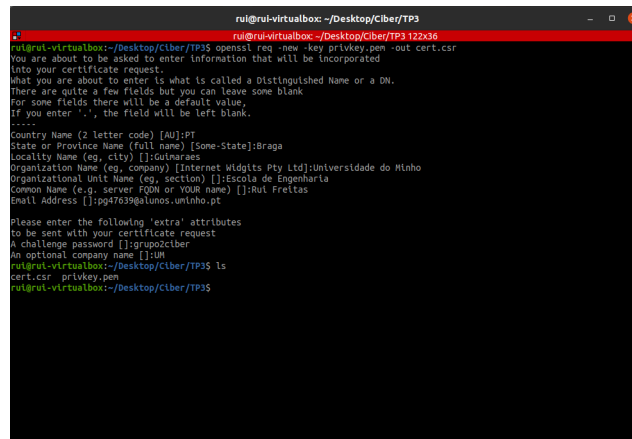
rul@rul-virtualbox: ~/Desktop/Ciber/TP3
rul@rul-virtualbox:~/Desktop/Ciber/TP3$ openssl rsa -in privkey.pem -check
writing RSA key
-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEAJw5JmKd0pJdyU5S8uA8e7PKEp9hbf+c8YelwJUT
SbuiTP6wRtCtW9F9PHLDDenVtQF9Q/+qf/bCk2T584IEEXwJ0ATjCjXKerVAg3
HwKavKI3sVcr5V0LcyPLX05nJHk553yr4C2VhpnLH/xvr4C2MFe9Vnncdoz
be/s0MFBolDyZns3aavvXQqJqKfULens1Gb15Z96FYL208b5hmq8u7FFPu
01/nYqap669/rtrMS77uYJnLwKd0pJdyU5S8uA8e7PKEp9hbf+c8YelwJUT
sqQn+BP1Be7hpuJAKdzr0+VrmxYBwLWkxQIDAQABIAADPLKg7DBNUKQcC
tJ/hKv1Cn5D2W5as5VbCuxs1Q9K13Frq10Jm422J96enJFVAGPvCAu48K
1D/CIEbz+qpaSLDn8LUbo0f/n2E3KXQ5Fm7p+e1T0nFunf56o59F7wla6
9ncktd04CP+D0kjk3p+A2sEwla9VL9GennDk56YEDHrku4amE9qE4xJ1SpG
FFd6JmYmymAFv7L1K3CU0205ZC2BYEGPTQKIEEjGfCL342TKryCU0NNH4e
0x1T5tWxt+smwvYKc1CnF//4S8dKrqGE1P4809wL1NULvhtE8xv
tCkdrkCgyEA58+vcgrMeBv1b109+u0Hse8zv1bcn4804QLT64Cw/LTbean+T
z1OKfBuy7H0KILVX8AdqgZ85RIZfCk9TEBxNLHxyYhYuskwBHF3om2HPndt
WkE291p0atwF/jaw9hndf46okcs4F013UfZLc9yKdHwpmE8CgyASBK
00gyxX39TH/annFtkVhQ5rpbEbcBL0e1pexoST1xx3MhGwy3v/sUlybF90054E
s1r7N/gpUL4Pu4H5qossYWCABw0zrny1bTe/d4p+Q4H31CfztthpTBPH2tp
fYmP2JLL3Uuz+up3kdAP9Jk4tqgqHnclwGyB2m1t1kvs+Hngd80758
LZ8WwMpa1rZCysy1KAhSnen0tpTc39LkuyLG1Eq+sg0VEnr0VRZ1bsyzbeU8C
BRU3Grugv8G0a8hrv02TrH5K3231VnLTK5d/WK5CV/F0v2B18XCAdhNBK
08FmFAsK4L988X0wF0G0Q0L2NhddeJ/ZKdF01+5d1655s0FmKq0qth3N
wofg26H5VJkWE4gJXmBj40bZq23jK0/GU3awtQmEQ5abYmWZ12z/F1s2j/fb/a
BNLQ08zBA91fYnLEH3E7A9Y+JL2Nln7agwv15r+0N/CBIakZa0AccheLU0E
vYp2w089CQcmph051B045G5BBHq2b03beBa1EvZmEMLKX1ANV5ShwuhUo
tSETLEAST9ghrVVDuavUJ2X3K0VCyF3JauddQ01pvs3Th49KBPn/7DkVYt8n
VUw3mpU8FF7Lab40q5MF3nv+cdabT0G15V3a+xxfHkP3Uupn2NzW=
-----END RSA PRIVATE KEY-----
rul@rul-virtualbox:~/Desktop/Ciber/TP3$

```

**Figura 15:** Verificação do estado da chave privada.

- **Passo 15:**

Foi gerado o pedido do certificado utilizando o seguinte comando.



```

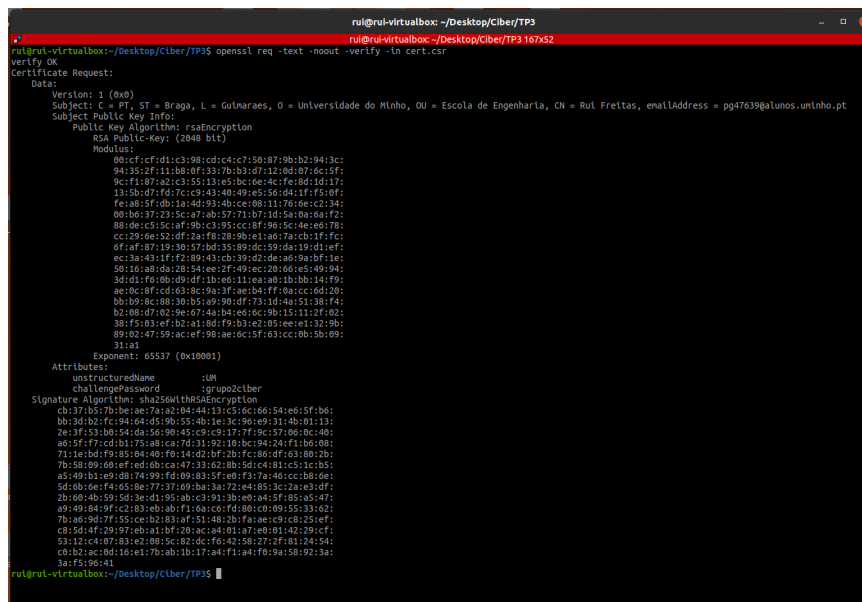
rui@rui-virtualbox: ~/Desktop/Ciber/TP3
rui@rui-virtualbox:~/Desktop/Ciber/TP3$ openssl req -new -key privkey.pem -out cert.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or 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) []:Guimarães
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Universidade do Minho
Organizational Unit Name (eg, section) []:Escola de Engenharia
Common Name (e.g. server FQDN or YOUR name) []:Rui Freltas
Email Address []:pg47639@alunos.unlho.pt

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:grupo2ciber
An optional company name []:UN
rui@rui-virtualbox:~/Desktop/Ciber/TP3$ ls
cert.csr  privkey.pem
rui@rui-virtualbox:~/Desktop/Ciber/TP3$

```

**Figura 16:** Criação do pedido de certificado.

Após a criação do pedido de certificado foi verificado o estado do ficheiro através do comando seguinte.



```

rui@rui-virtualbox: ~/Desktop/Ciber/TP3
rui@rui-virtualbox:~/Desktop/Ciber/TP3$ openssl req -text -noout -verify -in cert.csr
verify OK
Certificate Request:
Data:
  Version: 1 (0x0)
  Subject: C = PT, ST = Braga, L = Guimarães, O = Universidade do Minho, OU = Escola de Engenharia, CN = Rui Freltas, emailAddress = pg47639@alunos.unlho.pt
  Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
      RSA Public-Key: (2048 bit)
      Modulus:
        00:cfcfd1:c3:98:cd:c4:c7:50:87:9b:b2:94:3c:
        94:35:2f:11:b8:0f:33:7b:b3:d7:12:6d:07:6c:5f:
        9c:f1:07:a2:c3:53:e5:3b:ce:4c:fe:ed:1d:17:
        13:5b:d7:fd:7c:c9:43:40:49:e5:56:d4:1f:f5:0f:
        fe:a5:f7:db:1a:4d:93:4b:ce:08:11:76:0e:c2:34:
        00:b6:37:c3:5c:a7:ab:57:13:b7:1d:5a:0a:0a:f2:
        88:de:c5:5c:af:9b:c3:95:cc:8f:96:5c:4e:ed:78:
        cc:29:0e:52:0f:2a:f8:28:9b:e1:a6:7a:cb:1f:fc:
        4f:af:07:19:30:57:b5:35:09:dc:59:da:19:41:ef:
        ec:3a:43:1f:f2:89:43:cb:39:d2:de:ad:9a:bf:1e:
        5b:16:a8:da:28:54:ee:2f:49:ec:20:60:e5:49:94:
        34:d1:f6:0b:d9:df:1b:ed:11:ea:a0:1b:b6:14:f9:
        ae:0c:8f:cd:c6:8c:9a:3f:ae:b4:ff:0a:cc:6d:20:
        bb:b9:8c:88:30:b5:a9:90:df:73:1d:4a:51:38:f4:
        b2:08:d7:02:9e:07:4a:b4:e6:6c:9b:15:11:2f:02:
        38:f5:03:ef:b2:a1:8d:f9:b3:e2:05:ee:e1:32:9b:
        89:02:47:59:ac:ef:98:ae:6c:5f:63:cc:0b:5b:09:
        31:21
      Exponent: 65537 (0x10001)
  Attributes:
    unstructuredName : UN
    ChallengePassword : grupo2ciber
  Signature Algorithm: sha256WithRSAEncryption
    0b:37:b3:7b:be:ae:fa:a1:04:4b:1c:5c:06:54:ed:5f:b5:
    bb:3d:b2:fc:94:64:d5:9b:55:4b:1e:3c:9e:e9:31:4b:01:13:
    2e:3f:53:b0:54:da:56:90:45:c9:c9:17:7f:9c:57:06:0c:40:
    a0:5f:77:cd:b1:73:ad:ca:7d:31:92:1b:0c:94:24:f1:b6:08:
    71:ee:bdf:9b:85:04:4b:fa:14:01:b2:2b:fc:06:df:03:00:2b:
    7b:58:09:00:ef:ed:0b:ca:47:33:62:8b:5d:c4:81:c5:1c:b5:
    a5:49:b1:e9:d8:74:99:fd:09:b3:5f:eb:f3:7a:40:cc:b8:0e:
    5d:0b:0e:f4:65:0e:77:37:60:b3:3a:72:ee:a5:3c:2a:e3:df:
    2b:00:4b:59:5d:3e:d1:95:ab:c3:91:3b:eb:a4:5f:85:a5:47:
    a9:49:84:9f:c2:83:eb:ab:f1:6a:cd:fd:08:cb:09:55:33:62:
    7b:46:9d:7f:53:ce:b2:83:af:53:4b:2b:fa:ae:c9:c8:25:ef:
    c8:5d:4f:29:97:eb:a1:bf:20:ac:a4:01:a7:eb:01:42:29:cf:
    53:12:c4:07:b3:e2:08:5c:82:dc:fa:42:58:27:2f:81:24:54:
    c0:b2:ac:0d:16:e1:7b:ab:1b:17:a4:f1:a4:7b:9a:58:92:3a:
    3a:f5:96:41
rui@rui-virtualbox:~/Desktop/Ciber/TP3$

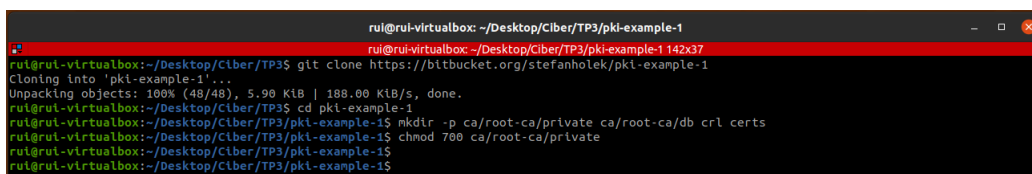
```

**Figura 17:** Verificação do estado do pedido de certificado.



- **Passo 17:**

Relativamente à autoridade de certificação foi decidido pelo grupo realizar a nossa própria implementação baseada num tutorial, encorajado pelo docente, para que o grupo obtivesse uma melhor compreensão do funcionamento das autoridades de certificação. Inicialmente foi clonado um repositório com alguns ficheiros de exemplo e criou-se a *root* CA com diretorias onde vão ser guardados os CRLs e os certificados como demonstrado de seguida.



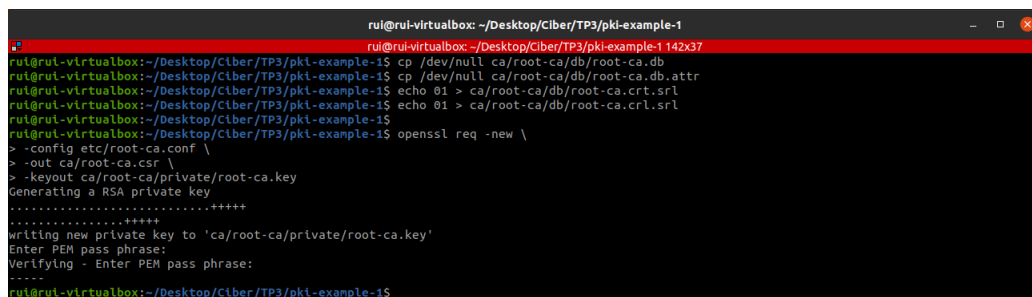
```

rui@rui-virtualbox: ~/Desktop/Ciber/TP3/pki-example-1
rui@rui-virtualbox:~/Desktop/Ciber/TP3$ git clone https://bitbucket.org/stefanhotek/pki-example-1
Cloning into 'pki-example-1'...
Unpacking objects: 100% (48/48), 5.98 KiB | 188.00 KiB/s, done.
rui@rui-virtualbox:~/Desktop/Ciber/TP3$ cd pki-example-1
rui@rui-virtualbox:~/Desktop/Ciber/TP3/pki-example-1$ mkdir -p ca/root-ca/private ca/root-ca/db crt certs
rui@rui-virtualbox:~/Desktop/Ciber/TP3/pki-example-1$ chmod 700 ca/root-ca/private
rui@rui-virtualbox:~/Desktop/Ciber/TP3/pki-example-1$
rui@rui-virtualbox:~/Desktop/Ciber/TP3/pki-example-1$

```

**Figura 20:** Criação do repositório e CA *root*.

Depois foram criadas as bases de dados e um CA *request* em que no *request* foi necessária a inserção de uma palavra chave para a *root* CA, como se pode verificar na figura 19.



```

rui@rui-virtualbox: ~/Desktop/Ciber/TP3/pki-example-1
rui@rui-virtualbox:~/Desktop/Ciber/TP3/pki-example-1 142x37
rui@rui-virtualbox:~/Desktop/Ciber/TP3/pki-example-1$ cp /dev/null ca/root-ca/db/root-ca.db
rui@rui-virtualbox:~/Desktop/Ciber/TP3/pki-example-1$ cp /dev/null ca/root-ca/db/root-ca.db.attr
rui@rui-virtualbox:~/Desktop/Ciber/TP3/pki-example-1$ echo 01 > ca/root-ca/db/root-ca.crt.srl
rui@rui-virtualbox:~/Desktop/Ciber/TP3/pki-example-1$ echo 01 > ca/root-ca/db/root-ca.crl.srl
rui@rui-virtualbox:~/Desktop/Ciber/TP3/pki-example-1$
rui@rui-virtualbox:~/Desktop/Ciber/TP3/pki-example-1$ openssl req -new \
> -config etc/root-ca.conf \
> -out ca/root-ca.csr \
> -keyout ca/root-ca/private/root-ca.key
Generating a RSA private key
.....+++++
.....+++++
writing new private key to 'ca/root-ca/private/root-ca.key'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
rui@rui-virtualbox:~/Desktop/Ciber/TP3/pki-example-1$

```

**Figura 21:** Criação das bases de dados e realizado um CA *request*.

Com o *request* criado procedeu-se à criação de um certificado CA auto assinado que serve como base de confiança da PKI criada.

```

rui@rui-virtualbox: ~/Desktop/Ciber/TP3/pki-example-1
rui@rui-virtualbox: ~/Desktop/Ciber/TP3/pki-example-1 144x41
rui@rui-virtualbox:~/Desktop/Ciber/TP3/pki-example-1$ openssl ca -selfsign \
> -config etc/root-ca.conf \
> -in ca/root-ca.csr \
> -out ca/root-ca.crt \
> -extensions root_ca_ext
Using configuration from etc/root-ca.conf
Enter pass phrase for ./ca/root-ca/private/root-ca.key:
Check that the request matches the signature
Signature ok
Certificate Details:
  Serial Number: 1 (0x1)
  Validity
    Not Before: Mar 27 22:31:08 2022 GMT
    Not After : Mar 26 22:31:08 2032 GMT
  Subject:
    domainComponent           = org
    domainComponent           = simple
    organizationName          = Simple Inc
    organizationalUnitName    = Simple Root CA
    commonName                 = Simple Root CA
  X509v3 extensions:
    X509v3 Key Usage: critical
      Certificate Sign, CRL Sign
    X509v3 Basic Constraints: critical
      CA:TRUE
    X509v3 Subject Key Identifier:
      EA:AC:13:FB:C9:60:A5:FA:4D:10:73:AE:7E:74:D0:3D:75:78:75:4F
    X509v3 Authority Key Identifier:
      keyid:EA:AC:13:FB:C9:60:A5:FA:4D:10:73:AE:7E:74:D0:3D:75:78:75:4F
Certificate is to be certified until Mar 26 22:31:08 2032 GMT (3652 days)
Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
rui@rui-virtualbox:~/Desktop/Ciber/TP3/pki-example-1$

```

**Figura 22:** Criação de um certificado CA auto assinado.

Com a finalização desta primeira fase de criar o *root* CA passamos à criação da CA assinada com a criação das diretorias, bases de dados e um CA *request* como demonstrado na figura 15.

```

rui@rui-virtualbox: ~/Desktop/Ciber/TP3/pki-example-1
rui@rui-virtualbox: ~/Desktop/Ciber/TP3/pki-example-1 152x53
rui@rui-virtualbox:~/Desktop/Ciber/TP3/pki-example-1$ mkdir -p ca/signing-ca/private ca/signing-ca/db ca/signing-ca/crl certs
rui@rui-virtualbox:~/Desktop/Ciber/TP3/pki-example-1$ chmod 700 ca/signing-ca/private
rui@rui-virtualbox:~/Desktop/Ciber/TP3/pki-example-1$ cp /dev/null ca/signing-ca/db/signing-ca.db
rui@rui-virtualbox:~/Desktop/Ciber/TP3/pki-example-1$ cp /dev/null ca/signing-ca/db/signing-ca.db.attr
rui@rui-virtualbox:~/Desktop/Ciber/TP3/pki-example-1$ echo 01 > ca/signing-ca/db/signing-ca.crt.srl
rui@rui-virtualbox:~/Desktop/Ciber/TP3/pki-example-1$ echo 01 > ca/signing-ca/db/signing-ca.crl.srl
rui@rui-virtualbox:~/Desktop/Ciber/TP3/pki-example-1$ openssl req -new \
> -config etc/signing-ca.conf \
> -out ca/signing-ca.csr \
> -keyout ca/signing-ca/private/signing-ca.key
Generating a RSA private key
.....+++++
.....+++++
Writing new private key to 'ca/signing-ca/private/signing-ca.key'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
rui@rui-virtualbox:~/Desktop/Ciber/TP3/pki-example-1$

```

**Figura 23:** Criação das diretorias, bases de dados e de um CA *request*.

Com o pedido criado foi utilizado o comando seguinte para criar o certificado CA assinado pela *root* CA.



```

rui@rui-virtualbox:~/Desktop/Ciber/TP3/pki-example-1$ openssl ca \
> -config etc/root-ca.conf \
> -in ca/signing-ca.csr \
> -out ca/signing-ca.crt \
> -extensions signing_ca_ext
Using configuration from etc/root-ca.conf
Enter pass phrase for ./ca/root-ca/private/root-ca.key:
Check that the request matches the signature
Signature ok
Certificate Details:
    Serial Number: 2 (0x2)
    Validity
        Not Before: Mar 27 22:39:13 2022 GMT
        Not After : Mar 26 22:39:13 2032 GMT
    Subject:
        domainComponent           = org
        domainComponent           = simple
        organizationName          = Simple Inc
        organizationalUnitName    = Simple Signing CA
        commonName                = Simple Signing CA
    X509v3 extensions:
        X509v3 Key Usage: critical
            Certificate Sign, CRL Sign
        X509v3 Basic Constraints: critical
            CA:TRUE, pathlen:0
        X509v3 Subject Key Identifier:
            71:30:C4:80:7E:E1:FC:74:54:16:07:33:A1:E3:18:A5:03:B1:00:41
        X509v3 Authority Key Identifier:
            keyid:EA:AC:13:FB:C9:60:A5:FA:4D:10:73:AE:7E:74:D0:3D:75:7B:75:4F

Certificate is to be certified until Mar 26 22:39:13 2032 GMT (3652 days)
Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]:y
Write out database with 1 new entries
Data Base Updated
rui@rui-virtualbox:~/Desktop/Ciber/TP3/pki-example-1$

```

**Figura 24:** Criação do certificado CA assinado pela *root* CA.

Com a criação da CA assinada é possível então utilizá-la para realizar um email *request* como demonstrado a seguir.

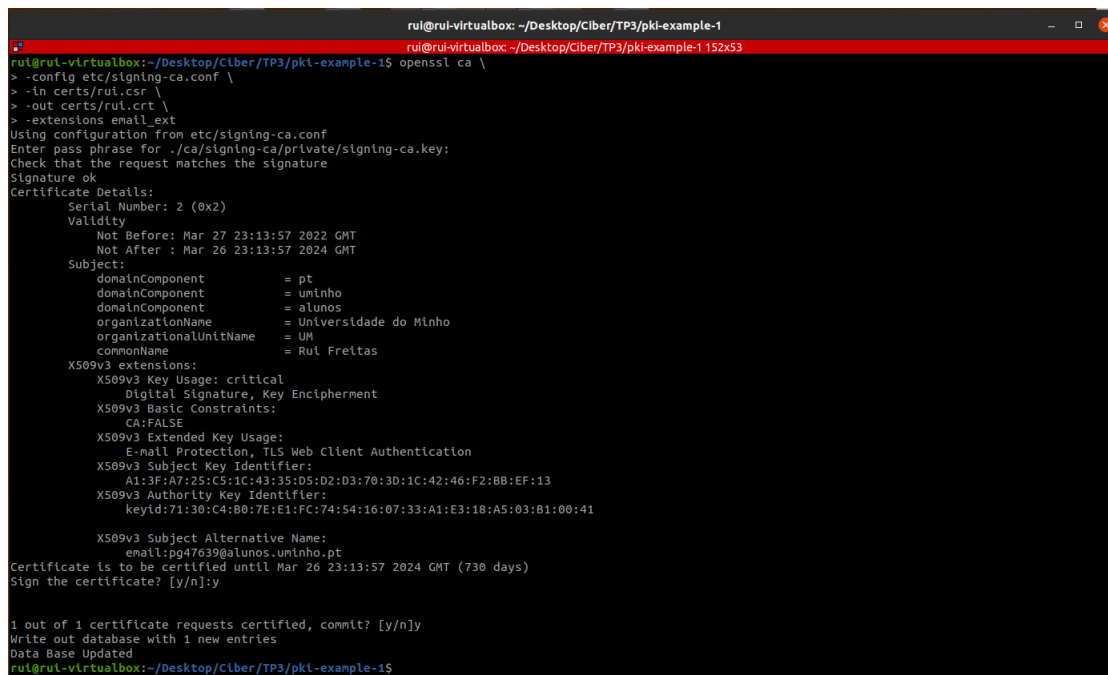
```

rui@rui-virtualbox: ~/Desktop/Ciber/TP3/pki-example-1
rui@rui-virtualbox: ~/Desktop/Ciber/TP3/pki-example-1 152x53
rui@rui-virtualbox:~/Desktop/Ciber/TP3/pki-example-1$ openssl req -new \
> -config etc/email.conf \
> -out certs/rui.csr \
> -keyout certs/rui.key
Generating a RSA private key
.....+++++
Writing new private key to 'certs/rui.key'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
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.
-----
1. Domain Component          (eg, com)          []:pt
2. Domain Component          (eg, company)   []:uminho
3. Domain Component          (eg, pk)          []:alunos
4. Organization Name         (eg, company)   []:Universidade do Minho
5. Organizational Unit Name  (eg, section)  []:UM
6. Common Name               (eg, full name) []:Rui Freitas
7. Email Address              (eg, name@fqdn) []:pg47639@alunos.uminho.pt
rui@rui-virtualbox:~/Desktop/Ciber/TP3/pki-example-1$

```

**Figura 25:** Realização do email *request*.

Após realizado o email *request* foi então criado o certificado do email.



```

rui@rui-virtualbox: ~/Desktop/Ciber/TP3/pki-example-1
rui@rui-virtualbox: ~/Desktop/Ciber/TP3/pki-example-1$ openssl ca \
> -config etc/signing-ca.conf \
> -in certs/rui.csr \
> -out certs/rui.crt \
> -extensions email_ext
Using configuration from etc/signing-ca.conf
Enter pass phrase for ./ca/signing-ca/private/signing-ca.key:
Check that the request matches the signature
Signature ok
Certificate Details:
  Serial Number: 2 (0x2)
  Validity
    Not Before: Mar 27 23:13:57 2022 GMT
    Not After : Mar 26 23:13:57 2024 GMT
  Subject:
    domainComponent      = pt
    domainComponent      = uminho
    domainComponent      = alunos
    organizationalName   = Universidade do Minho
    organizationalUnitName = UM
    commonName           = Rui Fretas
  X509v3 extensions:
    X509v3 Key Usage: critical
      Digital Signature, Key Encipherment
    X509v3 Basic Constraints:
      CA:FALSE
    X509v3 Extended Key Usage:
      E-mail Protection, TLS Web Client Authentication
    X509v3 Subject Key Identifier:
      A1:3F:A7:25:C5:1C:43:35:05:D2:D3:70:3D:1C:42:46:F2:BB:EF:13
    X509v3 Authority Key Identifier:
      keyid:71:30:C4:B0:7E:E1:FC:74:54:16:07:33:A1:E3:18:A5:03:B1:00:41

    X509v3 Subject Alternative Name:
      email:pg47639@alunos.uminho.pt
Certificate is to be certified until Mar 26 23:13:57 2024 GMT (730 days)
Sign the certificate? [y/n]:y

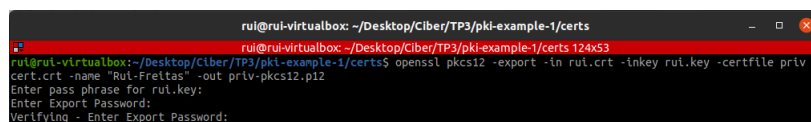
1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
rui@rui-virtualbox: ~/Desktop/Ciber/TP3/pki-example-1$

```

**Figura 26:** Criação do certificado email.

#### • Passo 18:

De modo a ser possível adicionar o certificado a diversas aplicações, é necessário criar um ficheiro no formato PKCS12, realizado como na figura abaixo.



```

rui@rui-virtualbox: ~/Desktop/Ciber/TP3/pki-example-1/certs
rui@rui-virtualbox: ~/Desktop/Ciber/TP3/pki-example-1/certs$ openssl pkcs12 -export -in rui.crt -inkey rui.key -certfile priv
cert.crt -name "Rui-Fretas" -out priv-pkcs12.p12
Enter pass phrase for rui.key:
Enter Export Password:
Verifying - Enter Export Password:

```

**Figura 27:** Criação do ficheiro no formato PKCS12.

Para verificar o estado do ficheiro com o certificado assinado e a chave privada foi utilizado o comando seguinte. Os elementos que consideramos mais relevantes neste ficheiro são a cadeia de certificados e a chave privada num único ficheiro encriptado. Relativamente à comparação dos elementos obtidos neste ficheiro com os obtidos no passo 4 é de notar que no passo 4 que foi onde foi criado o certificado auto assinado pela CA é possível obter informações sobre este certificado e alguns atributos como data de validade, entre outros, enquanto que no ficheiro no formato PKCS12 obtemos informação sobre a cadeia de certificados pelo qual o certificado passa para ser comprovado assim como a chave privada.



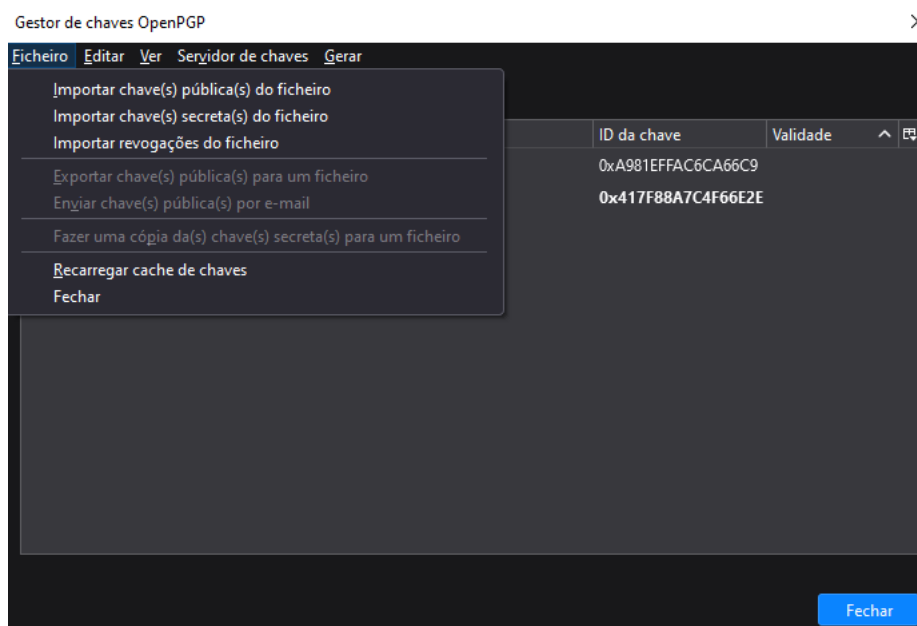
## 2 Enviar e receber mensagens seguras

### 2.1 Opção PGP

Para certificar os e-mails usando certificados PGP, foi necessário utilizar uma ferramenta já incluída no Thunderbird, o Gestor de Chaves OpenPGP. No enunciado foi aconselhado o uso de um add-on Enigmail para a adição dos certificados, mas este é obsoleto na versão atual do Thunderbird.

- **Passo 1:**

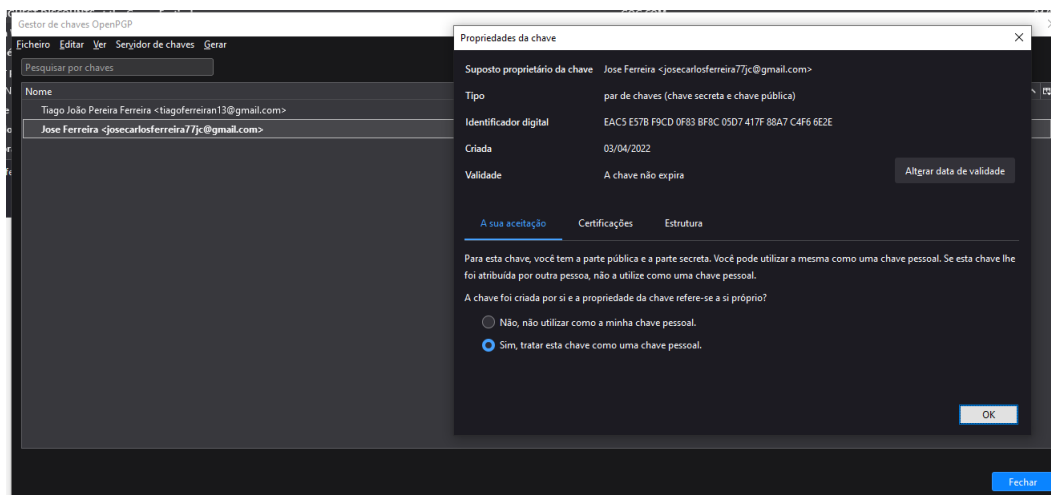
Na figura 30, representa-se o Gestor de chaves do OpenPGP aberto através das definições do Thunderbird onde na opção Ficheiro, vai ser importada a chave privada do utilizador para certificar o envio do e-mail e a chave pública do interveniente de quem queremos receber o e-mail.



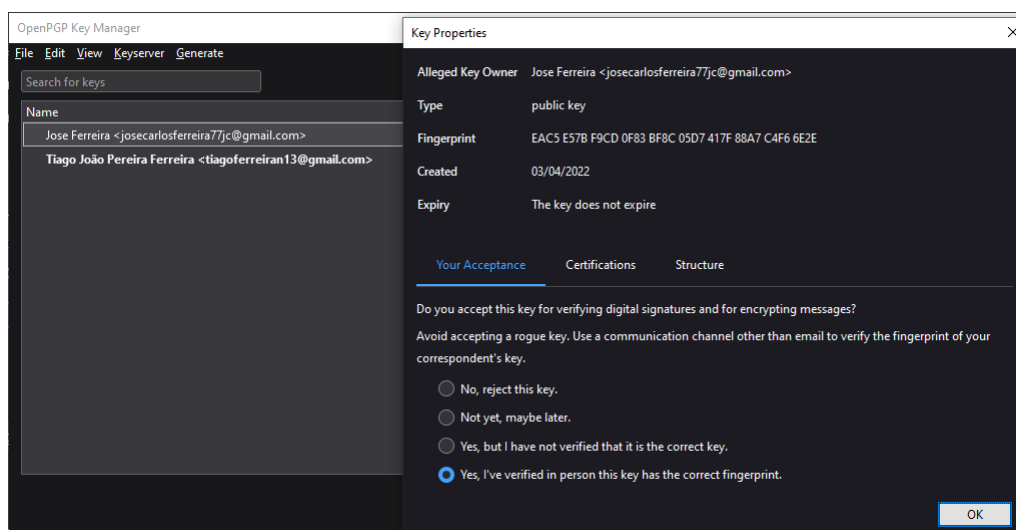
**Figura 30:** Inserir chaves públicas e privadas no Thunderbird.

- **Passo 2:**

Nas figuras 31 e 32 está a demonstração da adição no Thunderbird das chaves pública e privada dos alunos José e Tiago nos seus respetivos computadores.

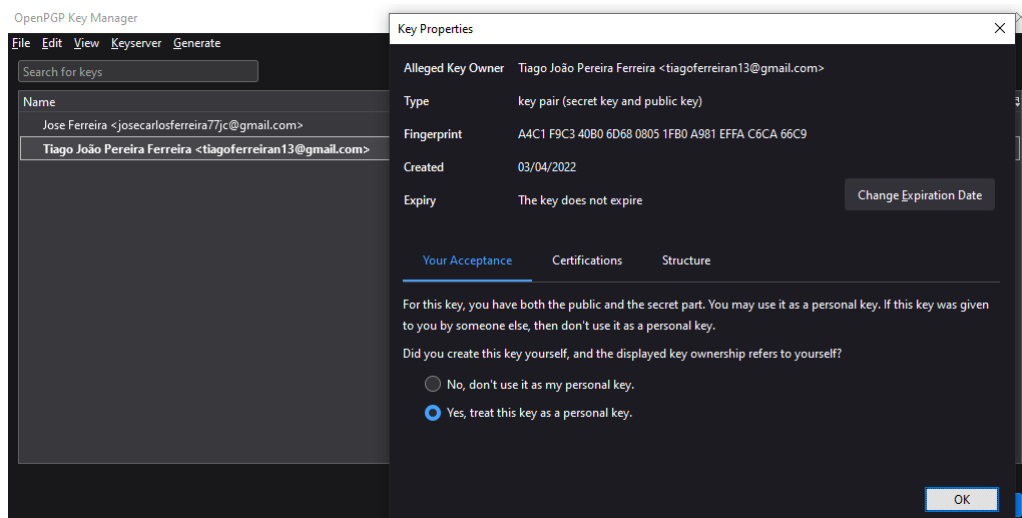


**Figura 31:** Importação da chave privada e pública do José.



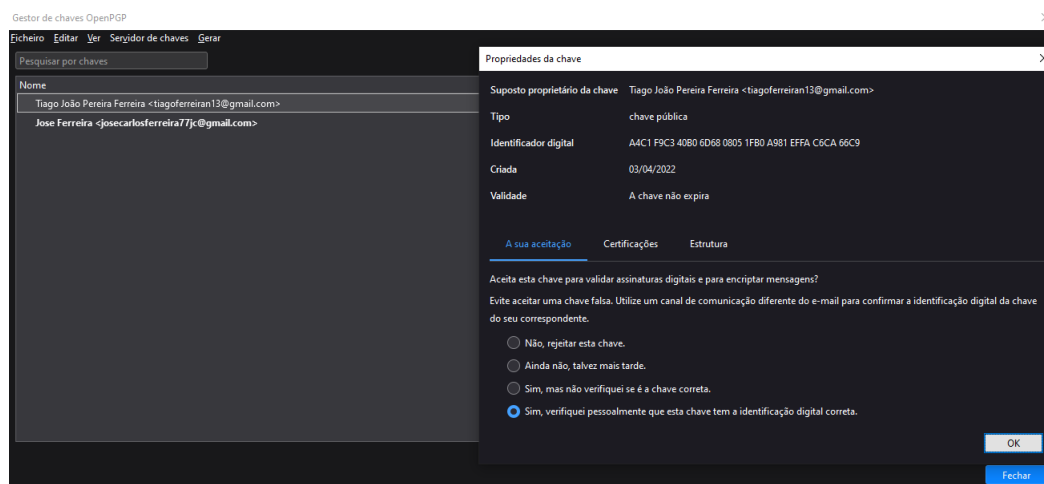
**Figura 32:** Importação da chave privada e pública do Tiago.

Na figura 33, é adicionado no Thunderbird do José a chave pública do Tiago.



**Figura 33:** Importação da chave pública do Tiago no Thunderbird do José.

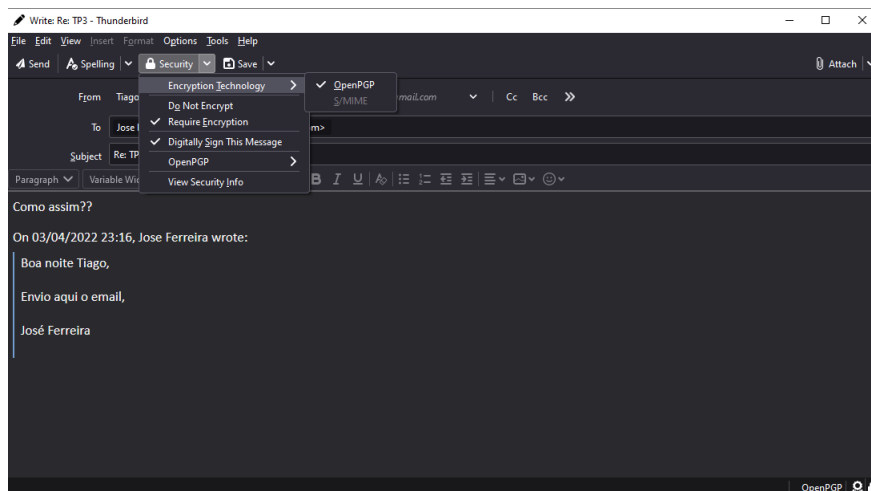
Na figura 34, é adicionado no Thunderbird do Tiago a chave pública do José.



**Figura 34:** Importação da chave pública do José no Thunderbird do Tiago.

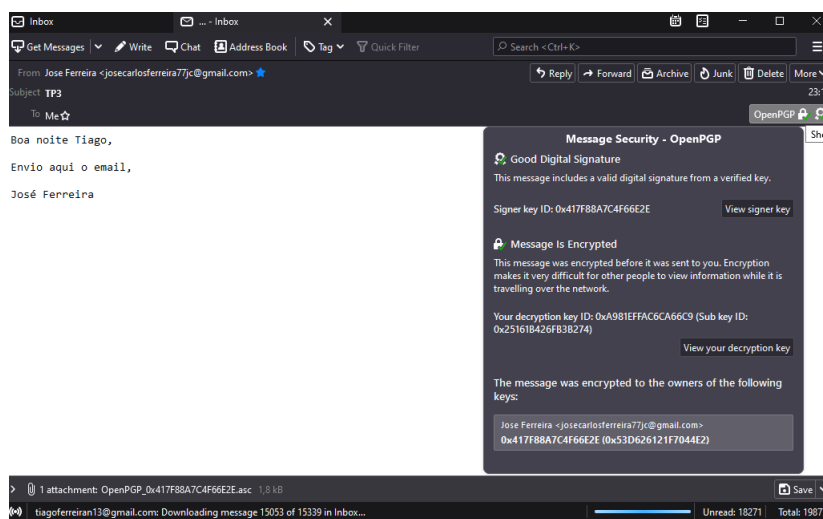
- **Passo 3:**

Para cifrar a mensagem na sua criação, é necessário ir à opção Security -> Encryption Technology e selecionar OpenPGP. É necessário também ativar as opções Require Encryption e Digital Sign This Message na opção Security, como demonstrado na figura 35.

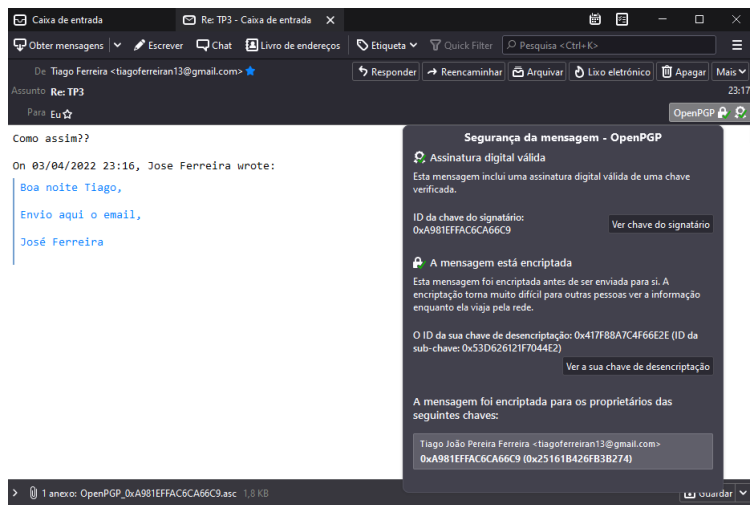


**Figura 35:** Exemplo de Envio de uma mensagem PGP.

Nas figuras 36 e 37 é demonstrado uma comunicação entre dois utilizadores com a confirmação de que a troca de e-mails está cifrada e assinada.



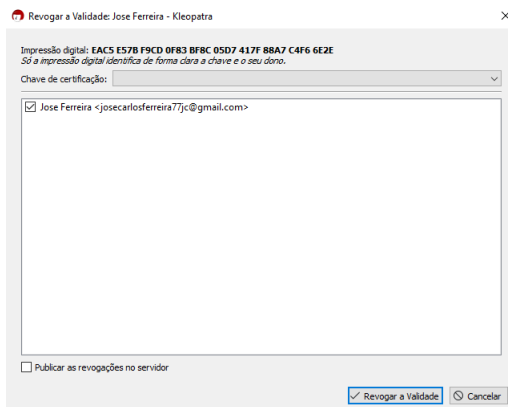
**Figura 36:** Receção da mensagem do José.



**Figura 37:** Receção da mensagem do Tiago.

- **Passo 4:**

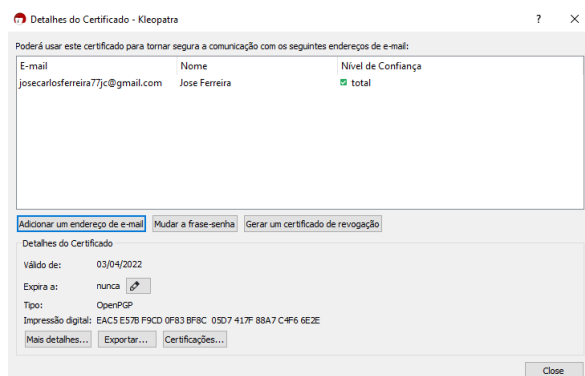
A revogação de chaves PGP foi feita de duas formas, uma utilizando apenas o Kleopatra, visível na figura 38, em que o envio dos e-mails no Thunderbird não é afetado.



**Figura 38:** Revogação no Kleopatra.

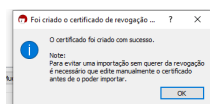
E outra em que é criado um certificado de revogação no Kleopatra, mostrado na figura 39, de forma a ser possível revogar as chaves no Thunderbird.





**Figura 39:** Geração do Certificado de Revogação.

Após ser gerado o certificado aparece um aviso de confirmação como se pode verificar na figura seguinte.



**Figura 40:** Confirmação da geração do certificado.

Na figura 41 pode ver-se o certificado de revogação após ter sido criado.

```

Este é um certificado de revogação para a chave de OpenPGP:

Jose Ferreira <josecarlosferreira77jc@gmail.com>
Fingerprint: EAC5E57BF9CD0F83BF8C05D7417F88A7C4F66E2E

Um certificado de revogação é uma espécie de "interruptor" para declarar
publicamente que uma chave já não deverá ser mais usada. Não é possível
voltar atrás com um destes certificados de revogação assim que for publicado.

Use-o para revogar esta chave, em caso de intromissão
ou perda da chave privada.

Para evitar um uso acidental deste ficheiro, foram adicionados dois-pontos
antes dos 5 traços abaixo. Remova este símbolo com um editor de texto antes
de importar e publicar este certificado de revogação.

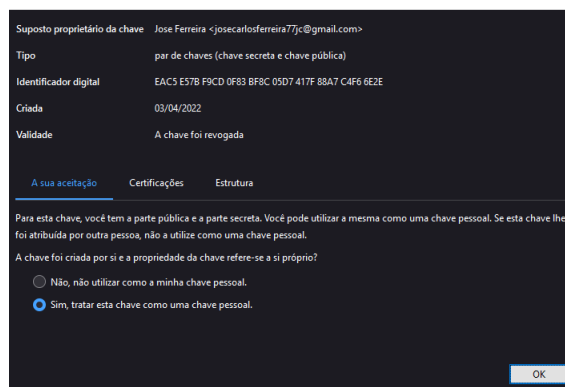
:-----BEGIN PGP PUBLIC KEY BLOCK-----
Comment: This is a revocation certificate

iQE2BCABCAAgFiEE6sX1e/nND40/jAXXQX+Ip8T2bi4FamJN8coCHQAACgkQQX+I
p8T2bi4iuQf7BwU7DVOQ5jreZiKtClzrvr1lERYQ+cFf13K2n7ssXMyPQVosgC4S
6tPUj0Xj+IcaL0ouMeA1omhJwRtRUQWb6tCkSCyULZ+5YSPazsnYGI1MFQU/zB9Ym
vjdo1Pvm060II13tFq0SEYZ+hwurkJG4+2xrkUwx9/cHF1LKwnIAYgGu4vytMX8
RPVSYIOs53oTcJchmU1Afqwvk+6N7V1u7et/6IGzU0W8SdISLZGsPNDzgy5Z+1ua
nRoaF09pnWAX/bk08BISa9Ef5tLg3u8GzP/HDpADcMKi1LgvVpa2xeSE0yKgA5MV
E+xA5n9P9jap+eB0Ia967bqAhWRmMpGS/A==
--LX57
-----END PGP PUBLIC KEY BLOCK-----

```

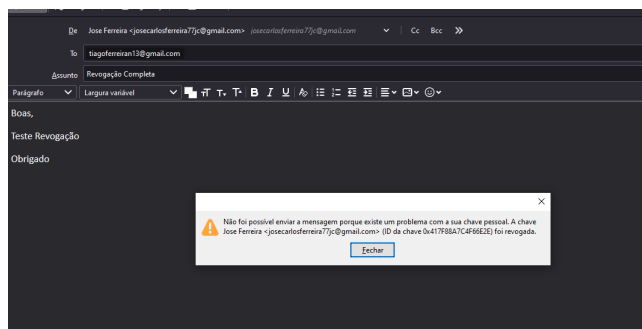
**Figura 41:** Certificado de Revogação.

Depois da criação do certificado de revogação, é possível adicioná-lo no Thunderbird, processo igual ao passo 1. Na figura seguinte pode ver-se a revogação da chave após a importação do certificado de revogação.



**Figura 42:** Chave Revogada no Thunderbird.

A revogação das chaves de um utilizador afeta o envio de e-mails do próprio, figura 43. No entanto, poderá na mesma receber e-mails uma vez que a chave pública do outro utilizador não foi revogada.

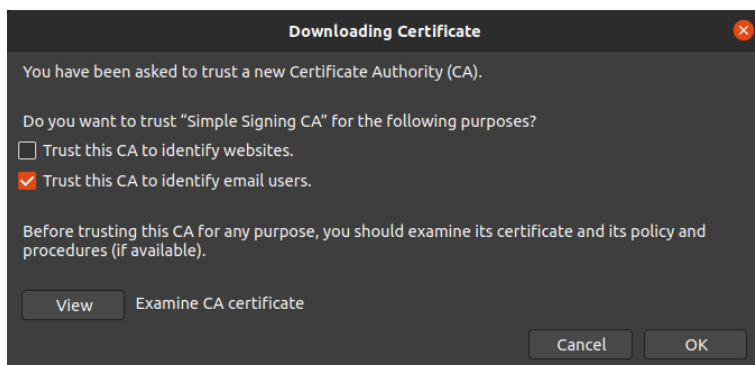


**Figura 43:** Tentativa de envio de um e-mail após revogação.

## 2.2 Opção X509

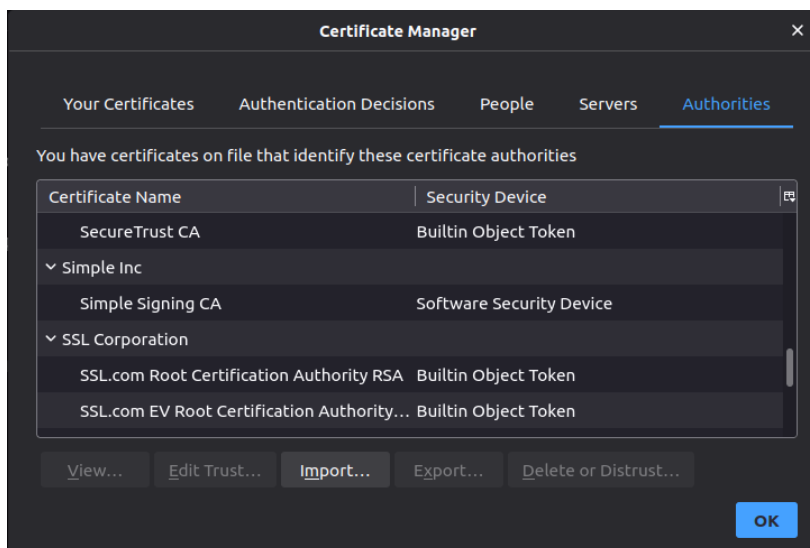
- **Passo 2a:**

De modo a podermos enviar e-mails de forma certificada por ambas as entidades foi necessário importar os certificados tanto do utilizador como da autoridade certificadora. Primeiramente importamos para o Thunderbird os certificados da autoridade certificadora como demonstrado a seguir.



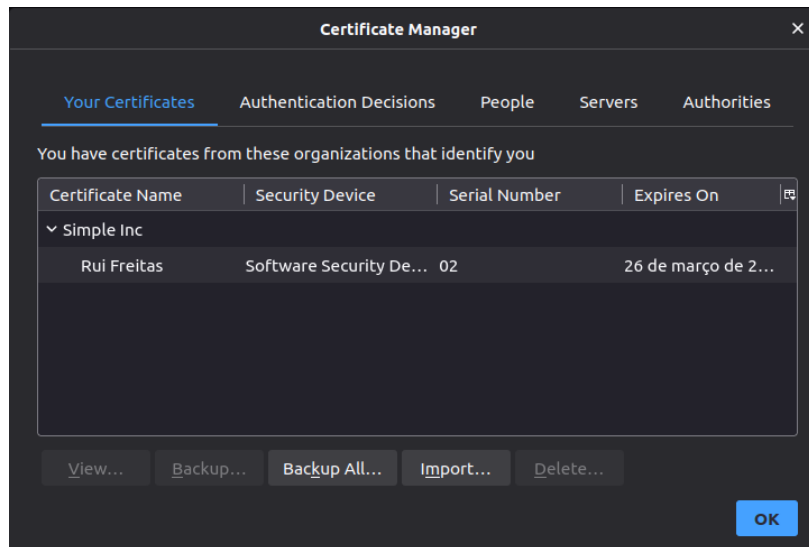
**Figura 44:** Importação do certificado da CA.

Após importarmos o certificado da CA foi necessário verificarmos a presença da autoridade criada na lista de autoridades aceites pelo Thunderbird como demonstrado de seguida.



**Figura 45:** Verificação do certificado da CA.

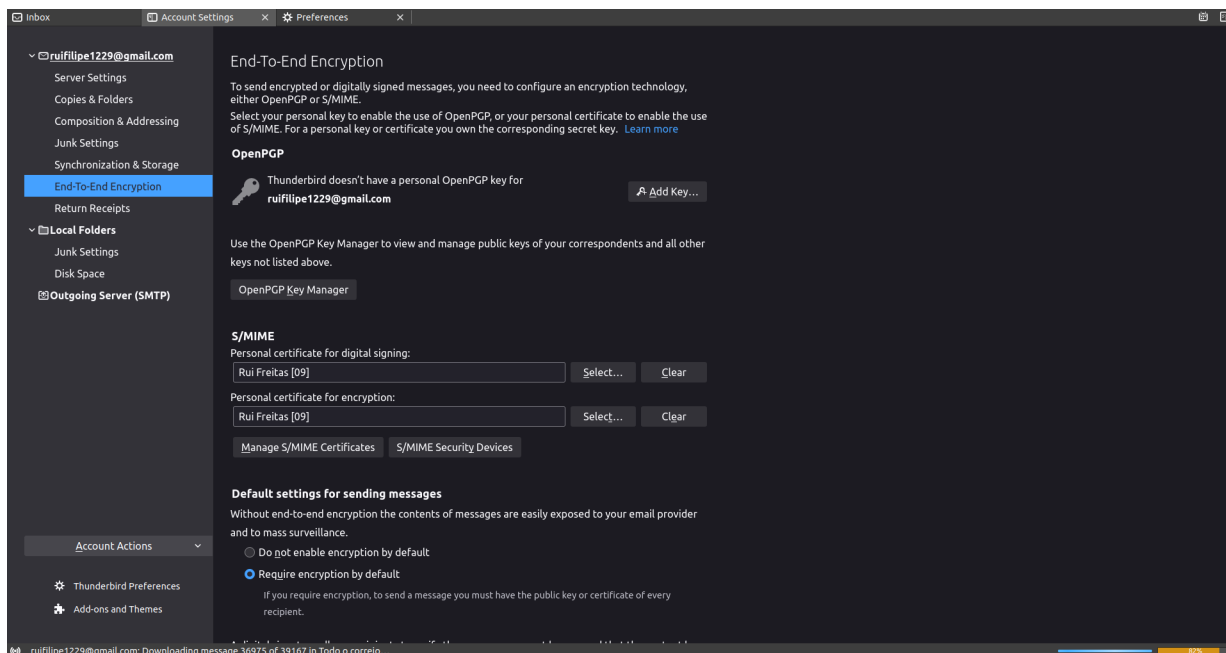
Com o certificado da CA adicionado foi necessário adicionar o certificado do utilizador demonstrado na figura seguinte.



**Figura 46:** Verificação do certificado do utilizador.

- **Passo 2b:**

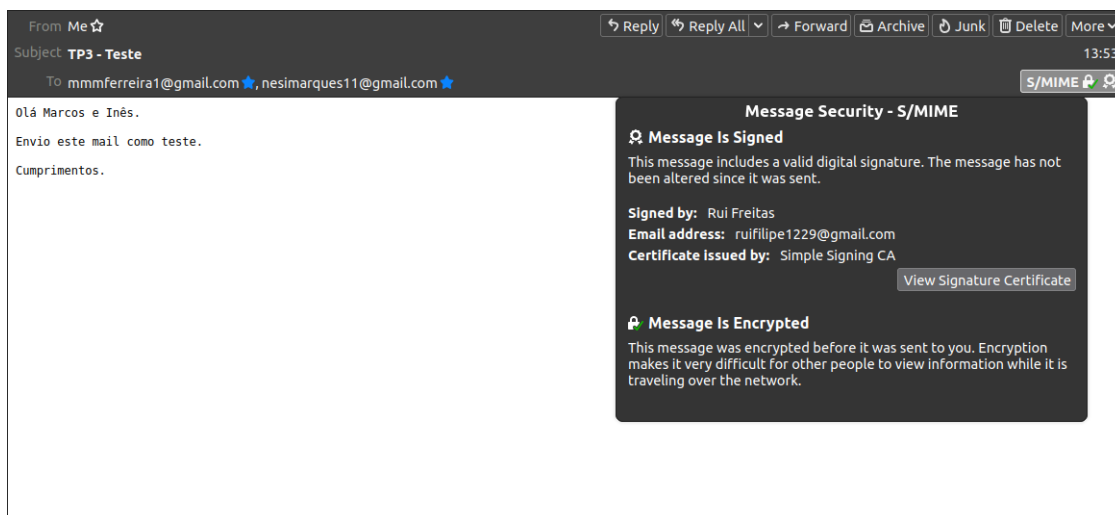
Neste passo escolhemos o certificado que pretendíamos utilizar para assinar e decifrar como demonstrado de seguida.



**Figura 47:** Configuração da assinatura digital.

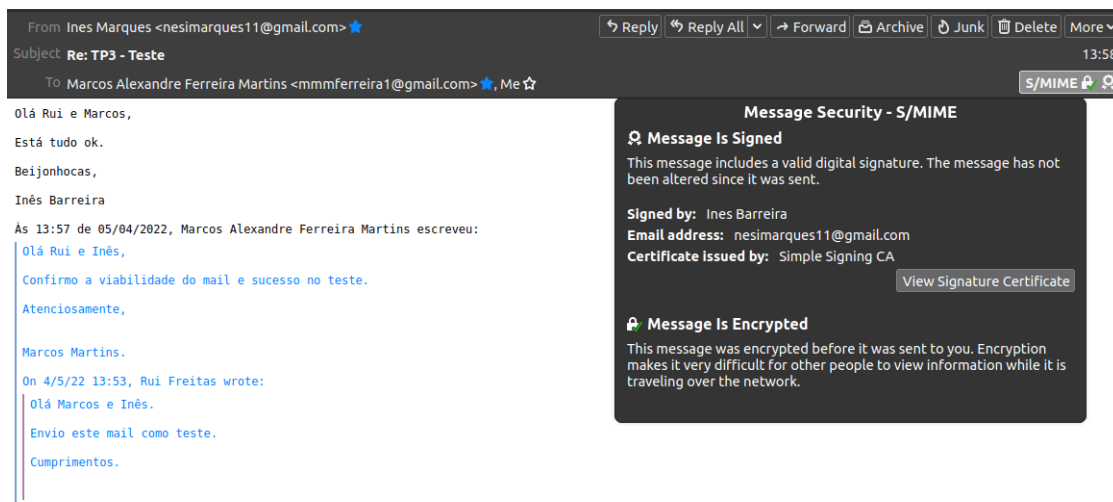
### • Passo 3:

De modo a comprovar a eficiência dos nossos certificados decidimos enviar e-mails entre os membros do grupo que possuíam os certificados X509. De seguida é demonstrado o envio de um e-mail com a assinatura correta e a mensagem encriptada.



**Figura 48:** Envio de um e-mail do Rui para o Marcos e Inês.

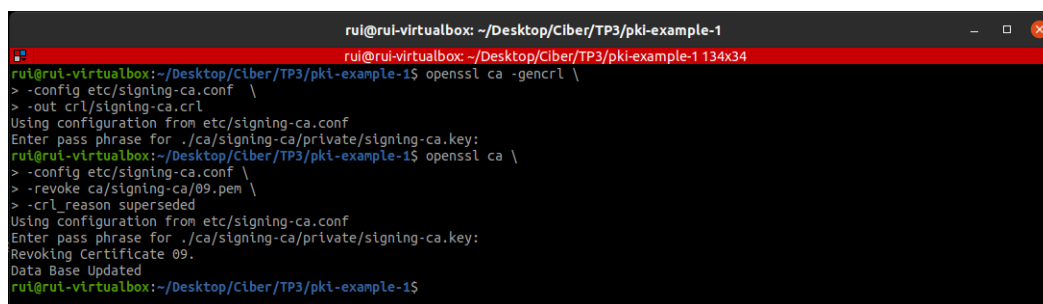
Após enviado o e-mail apresentado anteriormente foram enviadas mensagens por parte do Marcos e da Inês onde podemos verificar de seguida estas mensagens devidamente assinadas e encriptadas.



**Figura 49:** Receção dos e-mails do Marcos e da Inês.

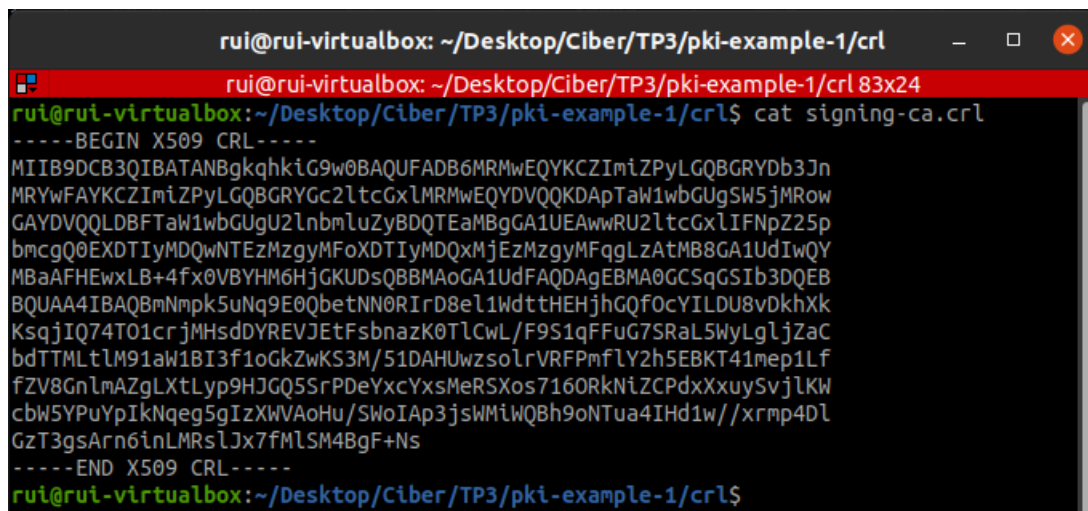
#### • Passo 4:

Para o passo 4 foi necessário realizar a revogação de um certificado e verificar o que acontecia. Primeiro foi criada uma lista CRL que vai conter os certificados revogados como demonstrado na figura seguinte. Após a criação da lista foi revogado o certificado com o segundo comando utilizado na imagem seguinte:



**Figura 50:** Revogação do certificado do Rui.

De modo a observar que a revogação foi realizada com sucesso basta acedermos à lista CRL como demonstrado a seguir.



```

rui@rui-virtualbox: ~/Desktop/Ciber/TP3/pki-example-1/crl
rui@rui-virtualbox: ~/Desktop/Ciber/TP3/pki-example-1/crl 83x24
rui@rui-virtualbox:~/Desktop/Ciber/TP3/pki-example-1/crl$ cat signing-ca.crl
-----BEGIN X509 CRL-----
MIIB9DCB3QIBATANBgkqhkiG9w0BAQUFADB6MRMwEQYKCZImiZPyLGBGRYDb3Jn
MRYwFAYKCZImiZPyLGBGRYGc2ltcGxLMRMwEQYDVQKDApTaw1wbGUgSW5jMR0w
GAYDVQQQLDBFTaw1wbGUgU2lnbmLuZyBDQTEaMBGGA1UEAwRU2ltcGxLIIFnpZ25p
bmcgQ0EXDTIyMDQwNTEzMzgyMFOxDTIyMDQxMjEzMzgyMFqgLzAtMB8GA1UdIwQY
MBaAFHEwxLB+4fx0VBYHM6HjGKUDsQBBMAoGA1UdFAQDAgEBMA0GCSqGSIb3DQEB
BQUAA4IBAQBmNmpk5uNq9E0QbetNN0RirD8el1WdtttHEHjhGQf0cYILDu8vDkhXk
KsqjIQ74T01crjMHsdDYREVJEtFsbnazK0TLCwL/F9S1qFFuG7SRaL5WyljZaC
bdTTMLtLM91aW1BI3f1oGkZwKS3M/51DAHUwzsolrVRFPmflY2h5EBKT41mep1Lf
fZV8GnlmAZgLTlYp9HJGQ5SrPDeYxcYxsMeRSXos7160RkNiZCPdxXxuySvjLKW
cbW5YPuYpIkNqeg5gIzXWVAoHu/SwoIAp3jsWmiWQBh9oNTua4IHd1w//xrmp4Dl
GzT3gsArn6inLMRsLJx7fMLSM4BgF+Nz
-----END X509 CRL-----
rui@rui-virtualbox:~/Desktop/Ciber/TP3/pki-example-1/crl$

```

**Figura 51:** Comprovativo da revogação do certificado.

Relativamente à revogação do certificado, este foi efetuado e incluído com sucesso na lista CRL da autoridade certificadora. Quanto à troca de mensagens com o certificado revogado não foi possível realizar, pois como o grupo realizou a sua própria entidade certificadora seria necessário uma maneira de atualizar as listas CRL no thunderbird, o que não é possível nas versões mais recentes. Outra alternativa era configurar um servidor OCSP mas como este se estava a tornar bastante complexo de implementar decidimos não o realizar.

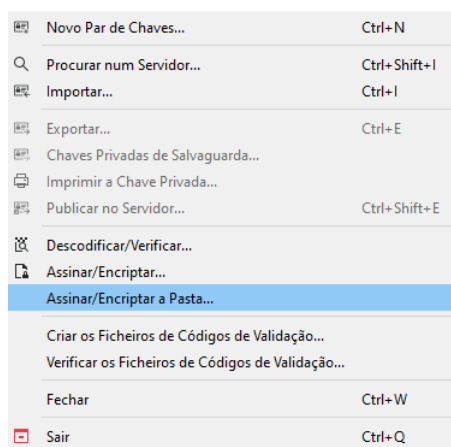
Uma das questões colocadas pelo docente foi de como resolveríamos o problema da certificação caso cada elemento do grupo tivesse implementado a sua própria CA. Como as CAs eram criadas localmente, para que todas se certificassem seria necessário haver uma root CA online que certificasse todas as CAs criadas, surgindo uma autoridade de topo auto assinada em que as root CAs previamente criadas deixariam de ser auto assinadas e seriam assinadas pela root CA criada online. Isto permitiria que quando um certificado realizasse um pedido de comprovação este passava pela cadeia de certificados até à root CA onde seria aprovado.

### 3 Proteger documentos locais

Para proteger documentos locais o Kleopatra oferece a possibilidade de assinar/cifrar pastas ou ficheiros. Para cifrar uma pasta foi necessário seguir os seguintes passos.

- **Passo 1:**

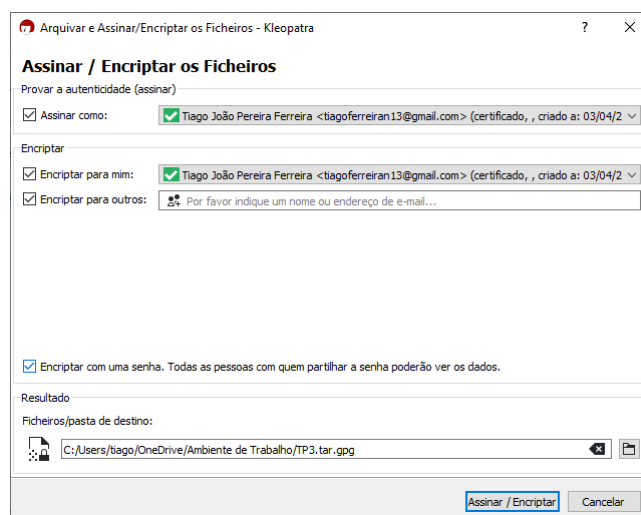
Selecionar a opção para cifrar a pasta.



**Figura 52:** Opção para assinar/cifrar a pasta.

- **Passo 2:**

Escolher o certificado a usar e a pasta desejada.

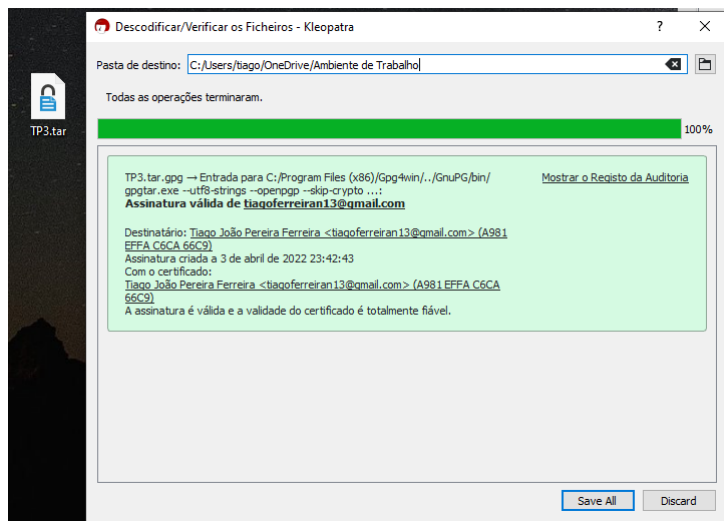


**Figura 53:** Escolha do certificado e pasta.



- **Passo 3:**

Para decifrar a pasta previamente cifrada apenas é preciso escolher a opção para decifrar e inserir a password.



**Figura 54:** Opção para decifrar a pasta.

## **4 Conclusão**

Para concluir, o grupo conseguiu alcançar o pretendido com o trabalho prático e ao mesmo tempo desenvolver competências de trabalho com certificados PGP e X509.

No PGP foram realizados todos os objetivos pretendidos, enquanto que no X509, não foi conseguida a confirmação da revogação no Thunderbird, uma vez que como a Autoridade de Certificação é local, isto faz com que não seja possível a atualização automática do estado do certificado.