



Universidade do Minho
Escola de Engenharia

Mestrado em Engenharia de Telecomunicações e Informática

Unidade Curricular de Cibersegurança

Docente: Henrique Santos

TP 3: Chaves de Cifra, Certificados e o PGP.

Bárbara Fonseca PG53677

Bruno Santos A93087

Camila Pinto PG53712

Eduarda Dinis PG53793

Gonçalo Dias PG53833

Guimarães, março de 2024

Índice de conteúdos

Índice de conteúdos	ii
Lista de Figuras	iii
Lista de acrónimos e siglas	vi
1. Introdução	1
2. Gestão de chaves	2
2.1 Opção PGP.....	2
2.2 Opção X509	10
3. Enviar e receber mensagens seguras.....	15
3.1 Opção PGP.....	15
3.2 Opção x509	19
4. Proteger documentos locais.....	24
5. Conclusão.....	27

Lista de Figuras

Figura 1. Criação de chave no <i>Kleopatra</i>	2
Figura 2. Configuração avançada da chave.	3
Figura 3. Certificações disponíveis.....	3
Figura 4. Chave pública.	4
Figura 5. Chave <i>master</i>	5
Figura 6. Criação de uma subchave para assinar.	5
Figura 7. Verificação da adição da subchave.....	6
Figura 8. Configuração do servidor.	6
Figura 9. Seleção do servidor e porta.....	7
Figura 10. Sucesso na importação.	7
Figura 11. Confirmação da chave no browser.	7
Figura 12. Confirmação da chave no Kleopatra.	8
Figura 13. Resultados da pesquisa por e-mail.	8
Figura 14. Resultados pesquisa por nome.....	9
Figura 15. Certificação da chave pública do colega.	10
Figura 16. Criação da chave privada.....	10
Figura 17. Criação de pedido de certificado.	11
Figura 18. Criação de um certificado auto-assinado.....	11
Figura 19. Site da CA.....	12
Figura 20. Certificado público da CA.....	12
Figura 21. Certificado assinado pela CA.	13
Figura 22. Certificado no formato PKCS#12.	13

Figura 23. Inserção das chaves públicas e privadas no Thunderbird.....	15
Figura 24. Propriedades da chave do utilizador.....	16
Figura 25. Propriedades da chave do interveniente.	16
Figura 26. Definição da chave dentro do Thunderbird para utilização.....	16
Figura 27. Configuração e envio de um e-mail encriptado e assinado.	17
Figura 28. Receção do e-mail encriptado e assinado.	17
Figura 29. Revogação da chave.	18
Figura 30. Confirmação da revogação da chave.	18
Figura 31. Chave revogada.	18
Figura 32. Rejeição do envio da mensagem.	19
Figura 33. Definições do Thunderbird.....	19
Figura 34. Certificate Manager, na aba Your Certificates.	20
Figura 35. Certificado no Thunderbird.	20
Figura 36. <i>Certificate Manager</i> , na aba <i>People</i>	20
Figura 37. Certificado público do recetor do e-mail.....	21
Figura 38. Confianças do CA.....	21
Figura 39. Encriptar e assinar.	22
Figura 40. S/MIME.....	22
Figura 41. E-mail pronto a enviar.	22
Figura 42. Envio da mensagem assinada e encriptada.....	23
Figura 43. Receção da mensagem assinada e encriptada.....	23
Figura 44. Encriptação do ficheiro.....	24
Figura 45. Sucesso na encriptação.	25
Figura 46. Sucesso na decifração.....	25
Figura 47. Encriptação do ficheiro.....	26

Figura 48. Sucesso na encriptação.	26
---	----

Lista de acrónimos e siglas

CA	Certificate Authority
PGP	Pretty Good Privacy
RSA	Rivest-Shamir-Adleman

1.Introdução

O presente relatório está a ser desenvolvido no âmbito da Unidade Curricular de Cibersegurança do 2º semestre do 1ºano do curso de Mestrado em Engenharia de Telecomunicações e Informática.

Neste terceiro trabalho prático, com o tema Chave de Cifra, Certificados e o PGP (*Pretty Good Privacy*), pretende-se compreender e descrever a forma como o conceito de chave pública é tipicamente implementado, reconhecer as operações associadas à gestão de chaves públicas e privadas, desenvolver competências na utilização de ferramentas de gestão de certificados e utilizar uma *framework* de criptografia para enviar e receber mensagens de e-mail, com segurança. 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.

2. Gestão de chaves

2.1 Opção PGP

Para implementar esta opção, foi instalado o gestor de certificados *Kleopatra* no ambiente Windows.

Passo 1: Criação de uma chave PGP, onde foram atribuídos nome e e-mail:

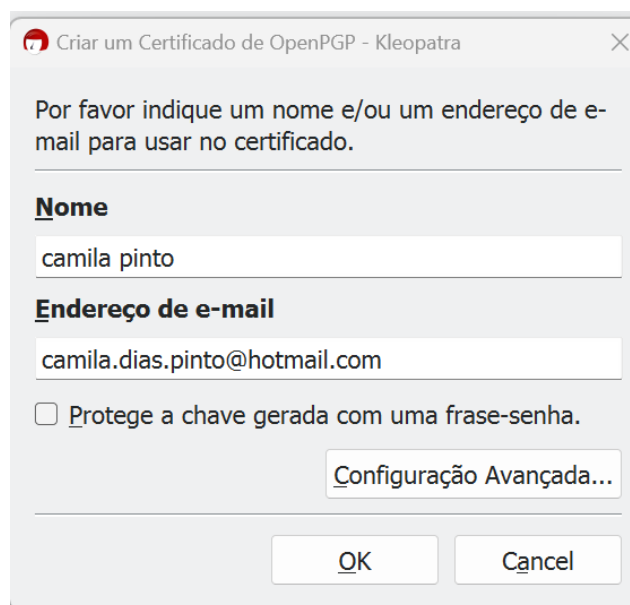


Figura 1. Criação de chave no *Kleopatra*.

Passo 2: Escolher o tipo de chave como RSA, com 2048 bits. O RSA utiliza um par de chaves: pública, para cifrar e privada para decifrar. Qualquer pessoa pode ter acesso à chave pública, mas a chave privada deve ser mantida em segredo.



Figura 2. Configuração avançada da chave.

Passo 3: Definir a *passphrase* como grupo4ciberseguranca, uma vez que é de fácil memorização.

Passo 4: Observando a Figura 4 notámos que a *fingerprint* está apresentada em formato hexadecimal. A chave representada nessa imagem é a chave pública, visto que está associada a uma *fingerprint* que pode ser usada para verificar a sua autenticidade. Após o cálculo do *hash* da mensagem, este vai ser assinado com a chave privada para assim criar a assinatura digital, que mais tarde será verificada com a chave pública, fazendo com que haja ligação entre a assinatura e a sua chave privada.

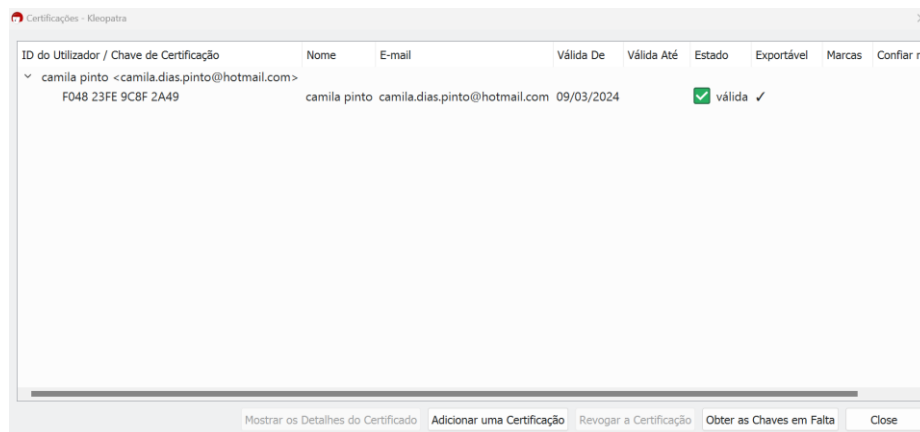


Figura 3. Certificações disponíveis.

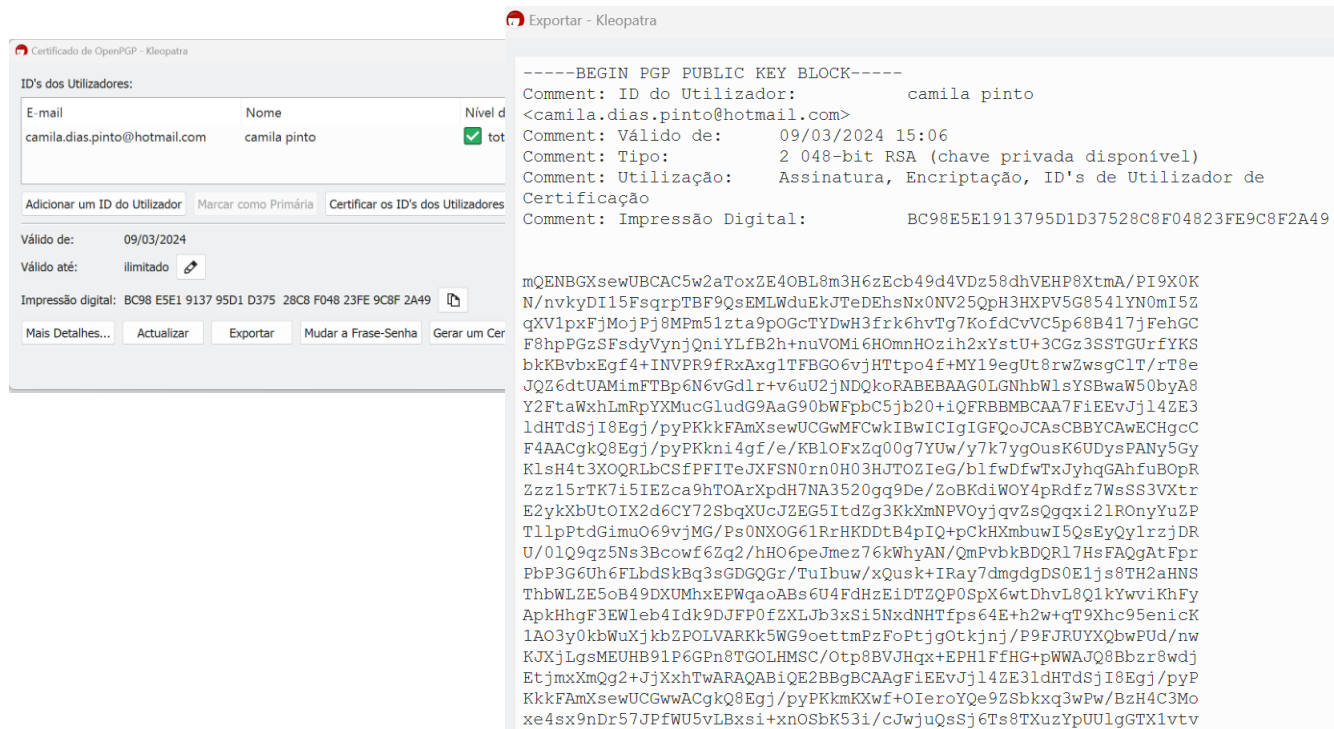


Figura 4. Chave pública.

Passo 5: Na Figura 5 é apresentada a chave *master*, usada para certificar e assinar e a subchave associada, usada apenas para encriptar. Dentro da chave master a parte privada é usada para assinar/certificar, por outro lado a parte publica é usada para validar a assinatura gerada. Na subchave, a parte pública é utilizada para cifrar os dados e a parte privada para decifrar.

A prática de associar subchaves a uma chave mestra surge da necessidade de preservar a confidencialidade da chave mestra. Ao criar subchaves específicas para funções individuais, como certificação, assinatura e criptografia, é possível manter a chave mestra em segredo enquanto se atribuem permissões distintas a cada subchave.

Por conseguinte, a associação de várias subchaves a uma chave, possui benefícios como por exemplo, se uma subchave for comprometida, apenas as funções associadas a essa subchave estão em risco, enquanto as outras permanecerão seguras; as subchaves podem ter prazos de validade independentes, permitindo a renovação e revogação de uma sem afetar outras.

Detalhes das Sub-Chaves - Kleopatra

Sub-chaves:

ID	Tipo	Válida De	Válida Até	Estado	Força	Utilização	Primária	Armazenamento
F048 23FE 9C8F 2A49	RSA	09/03/2024		boa	2048	Certificar, Assinar	✓	neste computador
801D 3702 9782 FF1F	RSA	09/03/2024		boa	2048	Encriptar		neste computador

Close

Figura 5. Chave *master*.

```

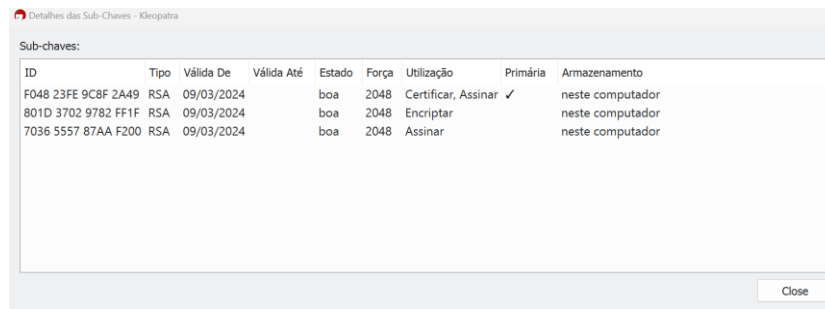
gpg> addkey
Selecione o tipo de chave desejado:
  (3) DSA (apenas de assinar)
  (4) RSA (apenas de assinar)
  (5) Elgamal (apenas de cifrar)
  (6) RSA (apenas de cifrar)
  (10) ECC (apenas de assinar)
  (12) ECC (apenas de cifrar)
  (14) Chave do cartão existente
Sua opção? 4
As chaves RSA podem estar entre 1024 e 4096 bits de comprimento.
Qual tamanho de chave você quer? (3072) 2048
O tamanho de chave pedido é 2048 bits
Especifique quando a chave expira.
  0 = chave não expira
  <n> = chave expira em n dias
  <n>w = chave expira em n semanas
  <n>m = chave expira em n meses
  <n>y = chave expira em n anos
Quando a chave expira? (0) 0
A chave não expira de forma alguma
Isto está correto? (s/N) s
De certeza que deseja criar? (s/N) s
Precisamos gerar muitos bytes aleatórios. É uma boa ideia realizar outra
atividade (escrever no teclado, mover o rato, usar os discos) durante a
geração dos números primos; isto dá ao gerador de números aleatórios
uma hipótese maior de ganhar entropia suficiente.

sec rsa2048/F04823FE9C8F2A49
criada: 2024-03-09 expira: nunca      uso: SC
confiança: plena      validade: plena
ssb rsa2048/801D37029782FF1F
criada: 2024-03-09 expira: nunca      uso: E
ssb rsa2048/7036555787AAF200
criada: 2024-03-09 expira: nunca      uso: S
[ plena ] (1). camila pinto <camila.dias.pinto@hotmail.com>
gpg> save

```

Figura 6. Criação de uma subchave para assinar.

Depois da criação da subchave, na Figura 7 é possível verificar que o processo foi bem-sucedido.



ID	Tipo	Válida De	Válida Até	Estado	Força	Utilização	Primária	Armazenamento
F048 23FE 9C8F 2A49	RSA	09/03/2024		boa	2048	Certificar, Assinar	✓	neste computador
801D 3702 9782 FF1F	RSA	09/03/2024		boa	2048	Encriptar		neste computador
7036 5557 87AA F200	RSA	09/03/2024		boa	2048	Assinar		neste computador

Figura 7. Verificação da adição da subchave.

Passo 6: Configurar o servidor, que vai ser utilizado para exportar a chave pública.

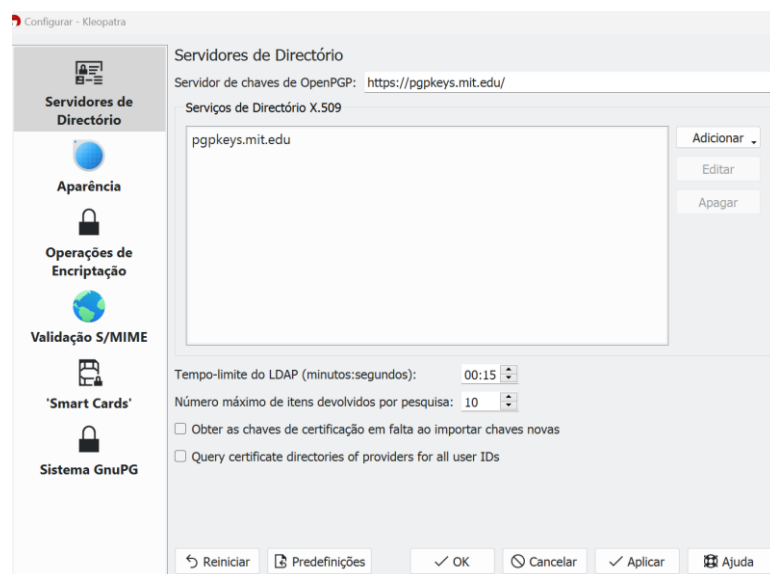


Figura 8. Configuração do servidor.

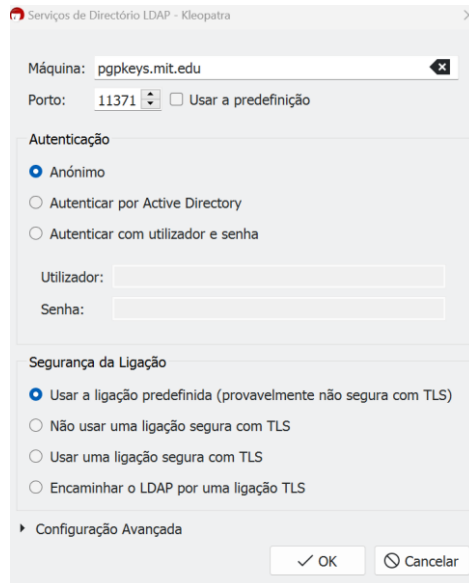


Figura 9. Seleção do servidor e porta.

Passo 7: Realizar a importação dos certificados para o servidor.

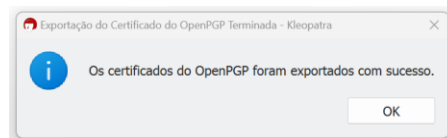


Figura 10. Sucesso na importação.

Passo 8: Confirmar a publicação da chave procurando-a no servidor através do *browser* e do *Kleopatra*.

Search results for 'pinto camila'

Type	bits/keyID	Date	User ID
pub	2048R/ 9C8F2A49	2024-03-09	camila pinto < camila.dias.pinto@hotmail.com >

Figura 11. Confirmação da chave no browser.

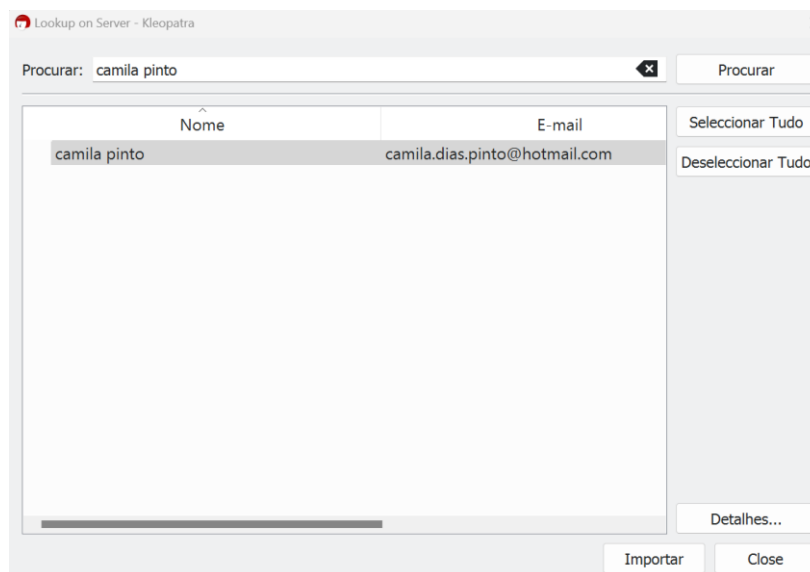


Figura 12. Confirmação da chave no Kleopatra.

Acedendo ao site *web* fornecido, pesquisados por nome e e-mail e obtivemos os resultados visíveis nas Figura 13 e Figura 14.

Search results for 'uminho pt hsantos dsi'

Type	bits/keyID	Date	User ID
pub	2048R/ 18A842EA	2018-11-01	Henrique M D Santos <henrique.dinis.santos@gmail.com> HSantos <henrique.dinis.santos@dsi.uminho.pt> Henrique Santos <henrique.dinis.santos@gmail.com>
pub	2048R/ 3473AE1C	2016-09-14	Henrique Santos (Chave para uso na UM) <hsantos@dsi.uminho.pt>
pub	1024D/ 475D4617	2006-07-13	Henrique M D Santos (No) <hsantos@dsi.uminho.pt>
pub	1024D/ 3AE27210	2003-11-14	*** KEY REVOKED *** [not verified] Henrique M D Santos <hsantos@dsi.uminho.pt> Henrique M D Santos (Para uso pessoal) <henrique.dinis.santos@gmail.com> [user attribute packet]
pub	1024D/ 319D3D84	2001-06-15	Henrique Manuel Dinis dos Santos <hsantos@dsi.uminho.pt>

Figura 13. Resultados da pesquisa por e-mail.

Search results for 'santos henrique'

Type	bits/keyID	Date	User ID
pub	3072R/49EEE789	2022-02-24	Paulo Henrique dos Santos <ownnerbr@gmail.com>
pub	3072R/26B2A788	2021-05-19	Henrique Santos <hfigueiredosantos@tecnico.ulisboa.pt>
pub	3072R/5DA4FEF	2021-05-17	alexandre henrique santos grisende <alexandre.grisende@aedb.br>
pub	3072R/D8EAD5D7	2021-05-17	alexandre henrique santos grisende <alexandre.grisende@aedb.br>
pub	2048R/EC68DAD8	2020-04-23	joao.h.santos@layer8.pt João Henrique Santos <joao.h.santos@layer8.pt>
pub	2048R/5E4588DA	2020-02-18	JORGE HENRIQUE SANTOS GARCEZ <mistergarcez@hotmail.com>
pub	2048R/18A842EA	2018-11-01	Henrique M D Santos <henrique.dinis.santos@gmail.com> HSantos <henrique.dinis.santos@dsi.uminho.pt> Henrique Santos <henrique.dinis.santos@gmail.com>
pub	2048R/86E90D28	2018-10-23	Henrique Santos <henrique.santos@inf.aedb.br>
pub	3072R/F3C5E85D	2018-08-29	Henrique dos Santos Goulart <henrique.goulart@chaordicsystems.com>
pub	1024D/E7598578	2018-06-12	Luiz Henrique Silva Santos <luizhenriqueeduardos@gmail.com>
pub	2048R/37F1E1F6	2018-05-16	Carlos Henrique dos Santos <kc-ny@hotmail.com>
pub	4096R/5EC3299C	2018-02-17	Launchpad PPA for Matheus Henrique dos Santos
pub	2048R/6B54B960	2018-02-17	Matheus Henrique dos Santos <vorf.dux@gmail.com>
pub	4096R/B4A4A88A	2016-10-26	Pedro Henrique Oliveira dos Santos (RELEASE SIGNING KEY) <pedro@apache.org>
pub	2048R/3473AE1C	2016-09-14	Henrique Santos (Chave para uso na UM) <hsantos@dsi.uminho.pt>
pub	4096R/618AD012	2016-05-20	Renan Henrique Santos da Silva <renanh2008@hotmail.com>
pub	1024R/7B4DCD73	2014-04-27	Rafael Henrique Santos Oliveira <rafael_pt@hotmail.com>
pub	1024D/4350FE61	2014-03-14	Jorge Branco (Prof Henrique Santos) <jorgebranco@iol.pt>
pub	4096R/D3490EC5	2011-04-15	Michel Henrique Aquino Santos (Chave Michel) <michel.has@gmail.com>
pub	2048R/8D78F998	2011-01-25	Pedro Henrique dos Santos <pedrohenrique@atlantico.com.br>
pub	2048R/99AA2678	2010-07-24	Paulo Henrique Andrade Domingues Rodrigues Santos (OAB/RJ 155991) <phads@gmail.com>
pub	1024R/CA6436DF	2010-03-18	Henrique M. D. Santos <henrique.dinis.santos@gmail.com>

Figura 14. Resultados pesquisa por nome.

Observando as figuras acima, repará-mos que a pesquisa por e-mail apresenta menos resultados comparativamente à pesquisa por nome. Isto ocorre, pois, as chaves públicas PGP geralmente estão associadas a identidades específicas, que podem incluir nomes, e-mail, etc. Enquanto o e-mail é um atributo único, o nome é mais comum aos utilizadores uma vez que estes podem usar variações do nome, bem como abreviações ou apelidos.

Passo 7: De forma a enviar a chave pública a um colega decidimos primeiramente exportar a chave pública, convertê-la em formato .txt e enviá-la para o endereço de e-mail de um colega. Para tal, o colega tem de cumprir todos os passos referidos anteriormente.

Após o *download* da chave pública recebida, esta foi importada e realizou-se o certificado, como demonstrado na Figura 15.

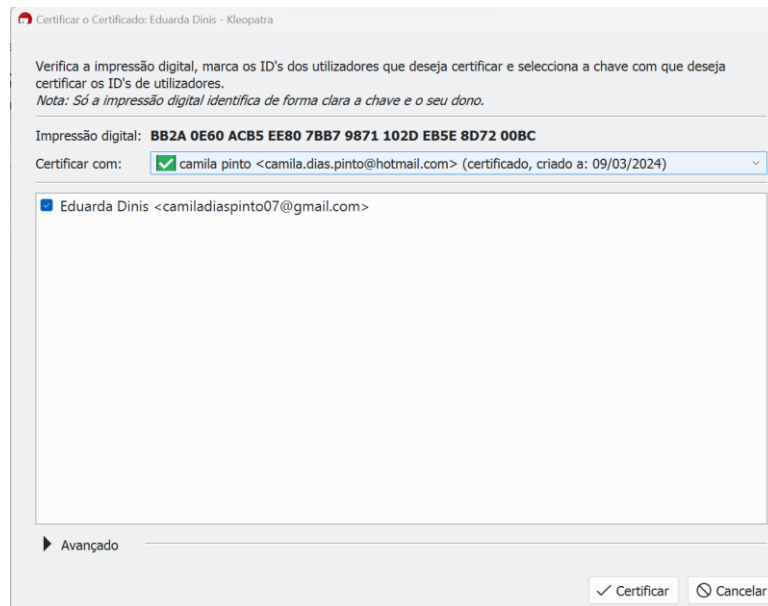


Figura 15. Certificação da chave pública do colega.

2.2 Opção X509

Para o desenvolvimento deste passo, o ambiente utilizado foi o Ubuntu que já continha nativamente a biblioteca Openssl, pelo que apenas foi verificada a versão.

Passo 1: Foi gerado um par de chaves, utilizando o comando disponibilizado no enunciado, de seguida utilizamos o comando representado na Figura 16 para verificar a chave privada.

```
edu@ubuntu-ciber:~/ciber$ openssl rsa -in eduarda.pem -check
RSA key ok
writing RSA key
-----BEGIN PRIVATE KEY-----
MIIEVQIBADANBgkqhkiG9w0BAQEFAASCBCwggSjAgEAAoIBAQRhtrS1EQu2afu
yyMF6EbV/uLNI0BoYBwnRjM6mX6OKMNCWZ/kbf9LzbG8pHb+ssrT0CBk4I39
Ixq8pgspPFcIqvaIzaQD9IlgsegrKxMU0FDHQbnb/6yGwTg//N4c5JWY2CosUqb4
JAKrARGY4Iv1819LUMtegyLHLJ+qbj1xhM9U705BqhvG/LyFBRnGdqEh742pLU
agRUxMR36C6ubX0NH14pks051wQxbU70yEg57kygDkudbtz8VRB+SSlreaRZ9w
daG6t1cHdzk0bEuckWq9LR7JkP7heAdE3me0d0C1BnPCGw0Z1tkqr5n/eczZd
e/Ad5HshagMBAACggEAFkyE0epE4gSK6+ZySa1a/go1g8sHMMrBN8tjffEh58sf
15EFV15CKISL/Kxknczy1tYUakrub1WY30f5UwvLLQftzFVlc8wmrZdKrfxvtpa0
9shJOCFmHwCYXGd0tdkD83JoBFXZzW7IV92kwIT9LP5rkZHuqSHGr52LLBoLavM
PGR00XU5jz8X8V8GjIfk04ZHVtQVga9JEHWoccsbNnLgFK9fC/tvF+pJRRfpzE
r/M+Ds/yZvLez10D0Hka0QXzFEJLVANb9vjp0Xu0z3fL/inSg+wq98jfuLVJ0dL
bvmJqectLgIc++ZN1Y5+LM33FhoFbgWl5srVZ42uQKBgQDnsE4kTWJ10XH1qJng
ZIAQ2UjTtyfuJNMtr3h08KM19/fby4ul3kFzDrUfK3QvXpGha54DJYtQ8nY9HTnN
yI8dqzXvEnm02pKPolrYsCUQ/7XRIAa0mJ140L2xTTV0a2j9waNfEBjCkT8ZUZ
HILWBunCKwZ5yHnI/+Ntst4TQKBgQDngzqqUL+9C2qBQAZb0ZINHwB/R1Vaix7
rP5ZeEMUB1ChCgkK99+1jNGX8ZT5bUMMo50vOPUXxckL3xtJP/02VCnBxUyNr
/CV308VlntRjPNR2ChmaE56Txyzm9q40PJeDQlVpFvtcoLGLHrpeEJQa1fz1wM
UbhxVWx4JQKBgQcj9QY3dnPYLQKlvxOKZDFW4TIK8XPgQb7nLjUWMOiZ5jcpWum
awja1M0nceoxFm1G3GBZLJRY2P9N7NE/MsaqdcGgmRYxNK2xqQXd/+jGFjmvY1
BPECj+KRjNko/yssP2Hp3B3seAW8WMB1C/0Kww93n/zbd3D76HPZ4eQKBgA3h
Hy5Aww35Vjx0c14jsckJiwluf/HK2LZIBGpnB3h0ZaFgKzU5UVySb70uUVLD
CP6od/0apZ9AoyGgcNL3Y523sDfCyZfZGQH8m6h9qIhZhdjFWxsln/ouEBITDeS
R0V+MJBvKzobu04rX9dJzZD5f8b/rnwKLl0t0uCFaogALqFokWfYd4THc7B1+YXa
zVDbacpmvjTdaJ+cgeVFqCX2VJUGzBcclLzNdcyWvSqp12Kjvm20WYK20mJKIXI
tNlp93VhrJ2X5cJbgJjmsHGtesGshSA9806KjXRATI1B4l/2oCPzLWLG2xQZbVJR
9WQhaQ9LXtZPBABId00TJw=
-----END PRIVATE KEY-----
```

Figura 16. Criação da chave privada.

Passo 2: Gerar um pedido de certificado e verificação do estado de pedido certificado após ser gerado, que inclui os atributos do pedido e do futuro certificado.

```

edu@ubuntu-ctber:~/ctber$ openssl req -text -noout -verify -in eduarda.csr
Certificate request self-signature verify OK
Certificate Request:
Data:
  Version: 1 (0x0)
  Subject: C = PT, ST = Braga, L = Guimaraes, O = UM, OU = EEUM, CN = eduarda, emailAddress = eduardadlns2204@gmail.com
  Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    Public-Key: (2048 bit)
    Modulus:
      00:d1:86:da:d2:d4:44:2e:d9:a7:ee:cb:23:05:33:
      a1:1b:57:fb:a5:34:83:81:a1:80:70:9d:12:66:ea:
      65:fa:38:a3:0d:ac:25:bc:07:f9:24:6d:ff:4b:cd:
      b1:bc:a4:76:fe:b2:ca:d3:d0:20:64:e0:8d:fd:23:
      1a:bc:a6:0b:29:3c:58:9c:22:ab:da:23:36:90:0f:
      d8:a0:b1:e8:2b:2b:13:14:d0:50:c7:40:19:db:ff:
      ac:86:c1:38:3f:fc:de:1c:48:95:98:64:2a:2c:52:
      a6:f8:8c:02:82:ac:04:46:63:82:2f:d7:c9:7d:2d:
      43:2d:7a:06:0b:1e:22:7e:aa:92:75:c6:13:3d:bb:
      b3:b9:05:08:0f:1b:f2:f2:14:14:67:19:da:84:96:
      1e:f8:da:99:54:6a:a4:5c:c4:77:e8:2e:ae:6d:
      7d:0d:1c:8e:29:92:c3:b9:d7:24:31:6d:4e:d0:c8:
      48:39:ee:4c:a0:0e:4b:9d:6e:dc:fc:55:10:7e:ad:
      2e:65:ad:ee:11:71:9f:70:75:a1:ba:b6:20:87:75:
      99:34:6c:45:1c:91:6a:b3:f4:b4:7b:24:aa:49:ee:
      17:80:74:4d:e6:78:e7:4e:08:80:66:3c:21:9c:c0:
      e6:75:b6:4a:ab:4a:7f:de:71:9b:1d:7b:f0:1d:48:
      7b:21
    Exponent: 65537 (0x10001)
  Attributes:
    unstructuredName      :eduarda
    challengePassword      :eduarda
    Requested Extensions:
    Signature Algorithm: sha256WithRSAEncryption
    Signature Value:
      a2:df:b6:85:89:4e:50:91:c5:3e:0a:acd4:0c:9c:a8:91:92:
      1a:3f:c2:9e:3a:89:2c:df:80:ab:8c:65:ec:e0:a6:3a:f2:59:
      d8:15:ca:b5:10:05:97:ff:90:61:0d:30:0c:66:e0:2b:7c:89:
      70:d2:6d:ef:2f:a4:f8:74:08:46:ab:19:f6:d2:10:53:d2:a0:
      8b:0c:1f:10:06:63:f0:7f:b5:51:3b:a1:bc:4b:c5:af:14:4e:
      c1:27:db:a4:49:e0:6f:9f:0c:f2:32:c3:55:32:68:a8:e4:
      56:89:53:3e:b7:8d:a7:d9:d5:af:86:b7:5f:a8:1d:6c:70:98:
      e6:6c:c9:86:e4:77:9b:78:2f:05:1a:84:e8:e4:9d:5f:d9:99:
      bd:c3:5c:18:5a:0b:b3:bb:4c:db:8e:97:47:d0:2f:b4:5c:5f:
      6d:fa:00:62:95:18:0e:db:fe:b9:8d:13:20:8e:a6:c1:e9:ca:
      34:51:e2:0c:f0:23:de:4d:9e:c3:ce:0b:bb:57:07:4b:e9:ba:

```

Figura 17. Criação de pedido de certificado.

Passo 3: Criação de um certificado auto-assinado e verificação do mesmo.

```

edu@ubuntu-ctber:~/ctber$ openssl x509 -text -in privcerteduarda.crt
Certificate:
Data:
  Version: 1 (0x0)
  Serial Number:
    11:f2:b2:d3:92:c7:e7:a7:fb:35:51:e6:f8:01:fa:33:41:3e:83:87
  Signature Algorithm: sha256WithRSAEncryption
  Issuer: C = PT, ST = Braga, L = Guimaraes, O = UM, OU = EEUM, CN = eduarda, emailAddress = eduardadlns2204@gmail.com
  Validity
    Not Before: Mar 22 15:31:41 2024 GMT
    Not After : Apr 21 15:31:41 2024 GMT
  Subject: C = PT, ST = Braga, L = Guimaraes, O = UM, OU = EEUM, CN = eduarda, emailAddress = eduardadlns2204@gmail.com
  Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    Public-Key: (2048 bit)
    Modulus:
      00:d1:86:da:d2:d4:44:2e:d9:a7:ee:cb:23:05:33:
      a1:1b:57:fb:a5:34:83:81:a1:80:70:9d:12:66:ea:
      65:fa:38:a3:0d:ac:25:bc:07:f9:24:6d:ff:4b:cd:
      b1:bc:a4:76:fe:b2:ca:d3:d0:20:64:e0:8d:fd:23:
      1a:bc:a6:0b:29:3c:58:9c:22:ab:da:23:36:90:0f:
      d8:a0:b1:e8:2b:2b:13:14:d0:50:c7:40:19:db:ff:
      ac:86:c1:38:3f:fc:de:1c:48:95:98:64:2a:2c:52:
      a6:f8:8c:02:82:ac:04:46:63:82:2f:d7:c9:7d:2d:
      43:2d:7a:06:0b:1e:22:7e:aa:92:75:c6:13:3d:bb:
      b3:b9:05:08:0f:1b:f2:f2:14:14:67:19:da:84:96:
      1e:f8:da:99:54:6a:a4:5c:c4:77:e8:2e:ae:6d:
      7d:0d:1c:8e:29:92:c3:b9:d7:24:31:6d:4e:d0:c8:
      48:39:ee:4c:a0:0e:4b:9d:6e:dc:fc:55:10:7e:ad:
      2e:65:ad:ee:11:71:9f:70:75:a1:ba:b6:20:87:75:
      99:34:6c:45:1c:91:6a:b3:f4:b4:7b:24:aa:49:ee:
      17:80:74:4d:e6:78:e7:4e:08:80:66:3c:21:9c:c0:
      e6:75:b6:4a:ab:4a:7f:de:71:9b:1d:7b:f0:1d:48:
      7b:21
    Exponent: 65537 (0x10001)
  Signature Algorithm: sha256WithRSAEncryption
  Signature Value:
    2f:7d:8f:8d:eb:ed:1a:90:b3:75:b6:e1:98:c3:5a:e6:8b:f0:
    61:64:0f:cc:29:24:f3:ed:21:6d:6d:65:2f:0b:1d:0c:22:2f:
    6c:94:9f:d9:e9:64:1b:d0:a5:e0:57:60:1d:22:a3:43:cc:db:
    15:04:9f:be:f4:f4:3d:77:12:0b:17:09:60:b0:4a:02:92:03:
    eb:1f:2c:f0:05:42:2c:db:e2:8c:84:2f:06:98:6c:a1:05:ae:
    08:a7:ba:9d:f7:13:0b:9c:0b:44:a1:97:ad:e2:56:bb:da:50:
    cb:f7:24:98:b4:49:1f:9a:a2:e5:c4:0b:a2:99:0b:d9:62:5f:
    09:81:98:85:61:68:bb:54:15:09:70:25:49:af:57:b3:42:c9:

```

Figura 18. Criação de um certificado auto-assinado.

Os elementos mais importantes de um certificado são o *Issuer*, que contém informação sobre quem emitiu o certificado, o *Subject* que contém informação sobre o responsável pelo certificado, o *Validity* que indica a validade do certificado e *Signature Algorithm* uma vez que revela informação sobre o algoritmo usado para a criação da assinatura, que é necessária para se poder validar e autenticar os certificados.

Passo 4: Este passo consiste em pedir um certificado público, devidamente assinado por uma CA (*Certificate Authority*). Utilizou-se o seguinte site dado pelo professor representado na Figura 19, que permite descarregar o certificado da CA, assinar um certificado com a CA e revogar um certificado.

CA certificate

Signing Service

Nenhum ficheiro selecionado

Revoking Service

Nenhum ficheiro selecionado

Figura 19. Site da CA.

Passo 5: Primeiramente descarregou-se o certificado público da CA.

```
edugubuntu-clber:~/clber$ cat cacert.crt
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            5c:0f:1d:e3:ad:74:05:38:55:43:d1:92:fe:3d:31:a0:fd:d9:b5:b4
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=PT, ST=Braga, O=Henrique Santos CA, OU=HS CA, CN=Henrique Santos
        CA/emailAddress=hsantos@dsi.uminho.pt
    Validity
        Not Before: Mar 18 01:09:09 2024 GMT
        Not After : Mar 18 01:09:09 2027 GMT
        Subject: C=PT, ST=Braga, O=Henrique Santos CA, OU=HS CA, CN=Henrique Santos
        CA/emailAddress=hsantos@dsi.uminho.pt
    Subject Public Key Info:
        Public Key Algorithm: rsaEncryption
        Public-Key: (2048 bit)
        Modulus:
            00:d6:40:6d:f0:c6:4f:df:32:94:0a:48:a2:82:13:
            6d:91:3c:39:97:15:5b:3a:d2:13:4e:d8:e7:d9:ec:
            10:56:3d:23:c7:fd:6c:d4:be:12:30:3e:06:7c:16:
            77:c5:36:26:75:8d:18:97:3e:26:a7:3f:d6:98:6d:
            53:36:ce:c8:47:9a:d1:e3:b9:29:2b:bb:0a:61:d0:
            d0:ba:5b:46:62:77:33:f6:00:07:8c:c4:3b:f1:1a:
            4e:38:46:34:87:ae:8e:ca:95:51:af:9c:9a:8b:47:
            bc:77:28:f9:82:bc:b4:65:59:6a:65:06:3a:c6:c3:
            5b:57:2e:c7:fb:9d:41:44:d2:ef:70:70:78:06:66:
            ed:d2:63:7d:ad:7a:0a:ba:b8:55:04:cf:8b:8c:08:
            66:7d:e9:a3:21:34:33:d3:94:12:16:fb:60:96:9f:
            de:a7:a5:5e:ff:58:01:d5:d5:58:54:6b:d7:ce:b2:
            0e:0e:c1:2d:bf:73:12:58:eb:08:1b:7e:3f:94:93:
            9b:69:19:80:e9:5e:59:1e:85:27:d3:e7:c6:95:fd:
            cc:23:5d:f8:77:39:b8:f8:d8:b1:1c:8e:ae:a4:85:
            d0:23:ee:85:e1:9a:99:a9:da:1b:d6:d7:ac:39:b2:
            a0:5d:40:88:67:1c:7e:8c:75:e9:09:39:83:44:6b:
            7b:9d
        Exponent: 65537 (0x10001)
    X509v3 extensions:
```

Figura 20. Certificado público da CA.

Gestão de Chaves

O certificado gerado no passo 6 é mais completo, incluindo informações sobre o certificado, a entidade certificadora e, possivelmente, a chave privada. Por outro lado, o certificado do passo 4 tem apenas informações sobre o próprio certificado e, se aplicável, sobre a entidade certificadora, além da chave pública.

A principal diferença é que o certificado do passo 6, assinado por uma CA, é mais confiável devido à validação pela CA. Isso estabelece uma cadeia de confiança reconhecida, enquanto o certificado autoassinado do passo 4 não passa por esse processo de validação externa.

3. Enviar e Receber Mensagens Seguras

3.1 Opção PGP

Para certificar os e-mails usando os certificados PGP, instalámos o Thunderbird, tal como recomendado, porém não utilizamos a extensão Enigmail uma vez que esta não é suportada pela versão atual do Thunderbird. Desta forma, foi utilizado o ambiente Windows, com Thunderbird e o gestor de chaves Open PGP.

Passo 1: Importar as nossas chaves públicas e privadas para o Thunderbird, através do gestor de chaves OpenPGP. Neste caso é importada a chave privada da Camila (utilizador) e a chave pública da Eduarda (interveniente), com quem queremos trocar e-mail.

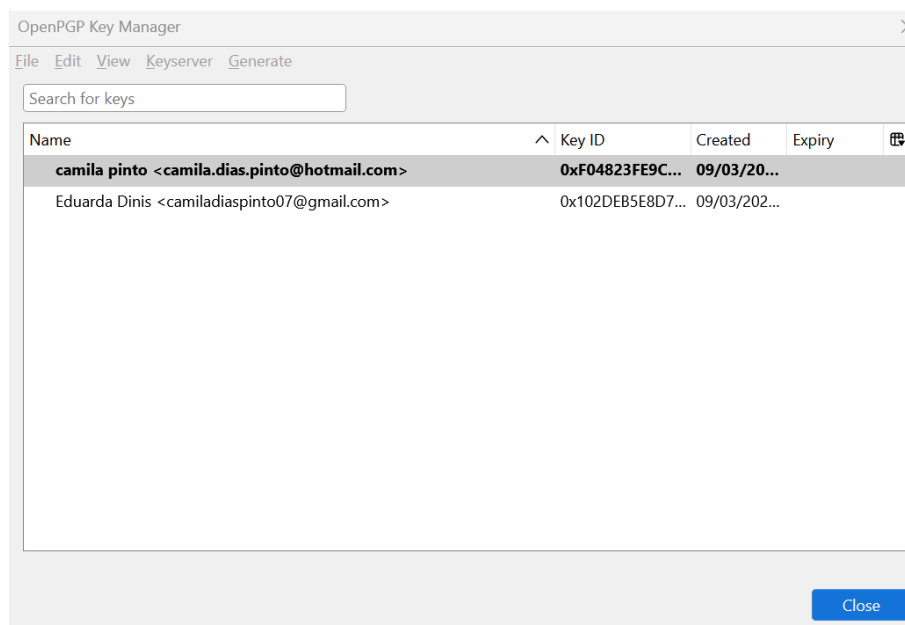


Figura 23. Inserção das chaves públicas e privadas no Thunderbird.

Key Properties

Claimed Key Owner

camila pinto <camila.dias.pinto@hotmail.com>

Type

key pair (secret key and public key)

Key ID

0xF04823FE9C8F2A49

Fingerprint

BC98 E5E1 9137 95D1 D375 28C8 F048 23FE 9C8F 2A49

Created

09/03/2024

Expiry

The key does not expire

Refresh Online

Change Expiration Date

Your Acceptance

Certifications

Structure

For this key, you have both the public and the secret part. You may use it as a personal key. If this key was given to you by someone else, then don't use it as a personal key.

☐ No, don't use it as my personal key.
 ☒ Yes, treat this key as a personal key.

Figura 24. Propriedades da chave do utilizador.

Key Properties

Claimed Key Owner

Eduarda Dinis <camiladiaspinto07@gmail.com>

Type

public key

Key ID

0x102DEB5E8D7200BC

Fingerprint

BB2A 0E60 ACB5 EE80 7BB7 9871 102D EB5E 8D72 00BC

Created

09/03/2024

Expiry

The key does not expire

Refresh Online

Your Acceptance

Certifications

Structure

Do you accept this key for verifying digital signatures and for encrypting messages?

☐ No, reject this key.
 ☐ Not yet, maybe later.
 ☐ Yes, but I have not verified that it is the correct key.
 ☒ Yes, I've verified in person this key has the correct fingerprint.

Verify the fingerprint of the key using a secure communication channel other than email to make sure that it's really the key of camiladiaspinto07@gmail.com.

OK

Cancel

Figura 25. Propriedades da chave do interveniente.

Passo 2: Seleção da chave a utilizar em cada computador.

OpenPGP

Thunderbird found 1 personal OpenPGP key associated with

camila.dias.pinto@hotmail.com

☒ Your current configuration uses key ID 0xF04823FE9C8F2A49
 [Saber mais](#)

Adicionar chave...

☐ Nenhuma

Não utilizar o OpenPGP para esta identidade.

☒ 0xF04823FE9C8F2A49

A chave não expira

Publishing the public key on a keyserver allows others to discover it.

Publish

Figura 26. Definição da chave dentro do Thunderbird para utilização.

Passo 3: Depois de termos importado e configurado as chaves necessárias, conseguimos enviar emails encriptados e assinados.

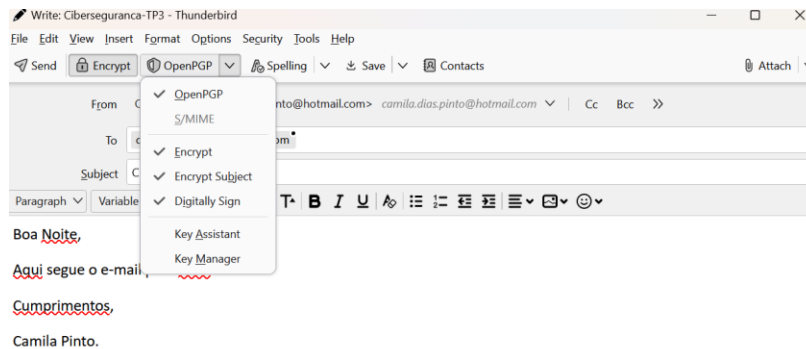


Figura 27. Configuração e envio de um e-mail encriptado e assinado.

Na Figura 28 verificámos a receção do e-mail por parte da colega de grupo devidamente encriptado e assinado.

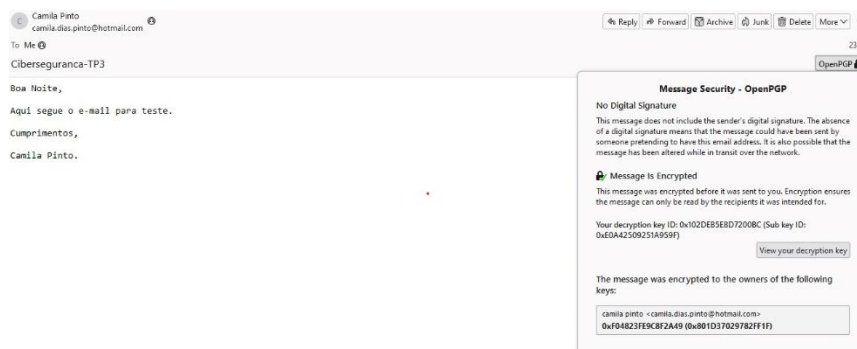


Figura 28. Receção do e-mail encriptado e assinado.

Passo 4: Ao revogar uma chave, pressupõe-se que a chave já não deverá mais ser utilizada e, portanto, já não seria possível enviar o e-mail. Para demonstrar isto podemos usar a ferramenta *Kleopatra*, ou pelo terminal criando um certificado revogado, neste caso optámos por utilizar a ferramenta.

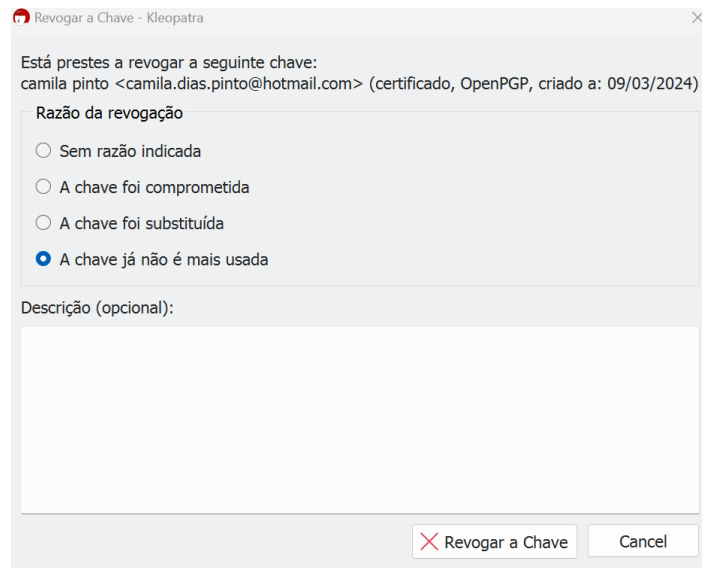


Figura 29. Revogação da chave.

Nome	E-mail	ID's do Utilizador	Válida De	Válida Até	ID da Chave
camila pinto	camila.dias.pinto@hotmail.com	revogada	09/03/...		F048 23F...
Eduarda Dinis	camiladiaspinto07@gmail.com	não certificado	09/03/2...		102D EB5E...

Figura 30. Confirmação da revogação da chave.

Passo 5: Importar a chave revogada no Thunderbird. Com a Figura 31 e verificado a data de validade verificamos que o certificado foi de facto revogado.

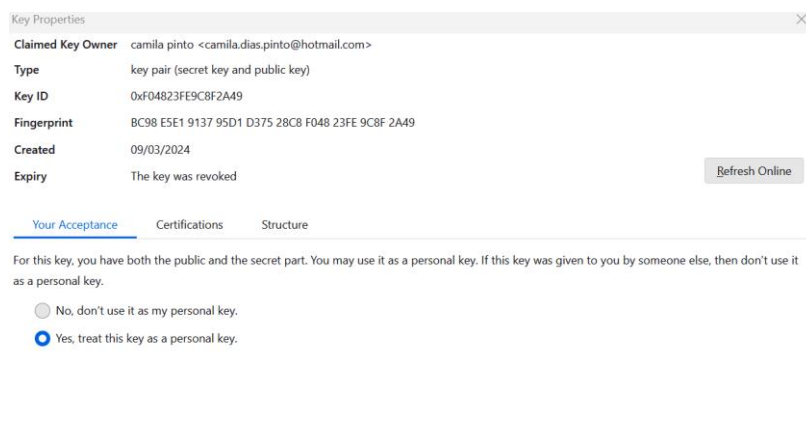


Figura 31. Chave revogada.

Passo 6: Verificar se não é permitido enviar e-mails, tal como pretendido. A Figura 32 mostra que o envio de e-mail não é permitido.

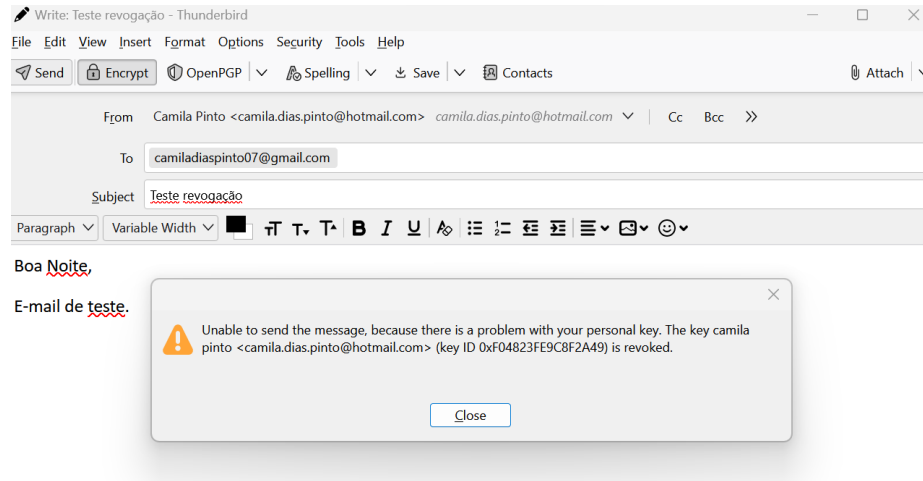


Figura 32. Rejeição do envio da mensagem.

3.2 Opção x509

Para o envio e receção de mensagens utilizou-se o Thunderbird.

Passo 1: De modo a importar os certificados x509 foi necessário aceder às definições do Thunderbird.

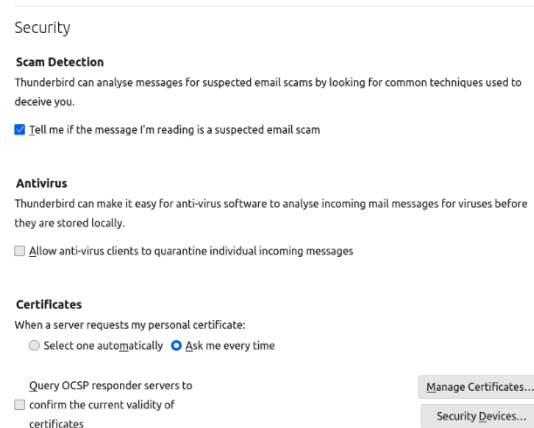


Figura 33. Definições do Thunderbird.

Passo 2: Adicionou-se o certificado na aba *Your Certificates* e o certificado do email recetor na aba *People*.

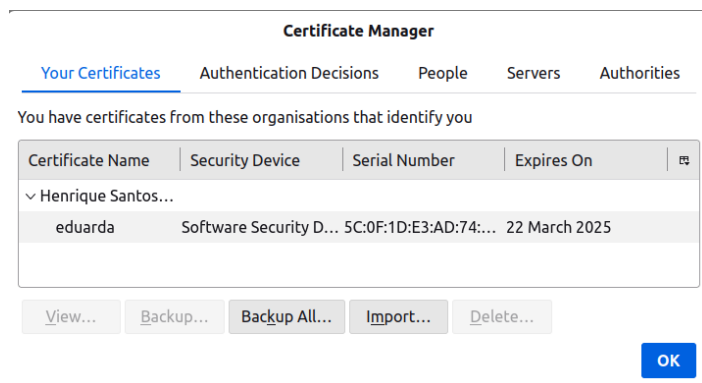


Figura 34. Certificate Manager, na aba Your Certificates.

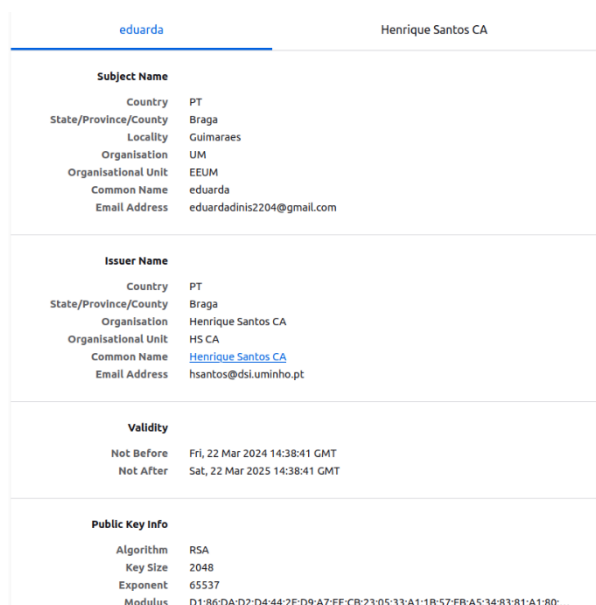


Figura 35. Certificado no Thunderbird.

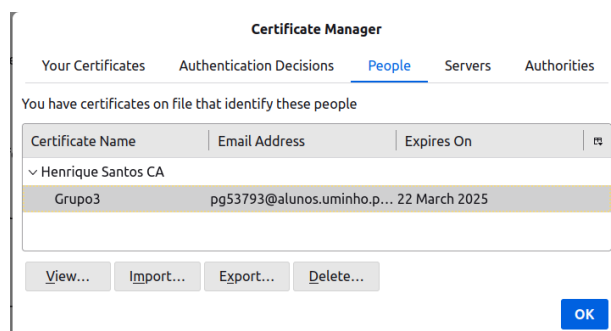


Figura 36. Certificate Manager, na aba People.

Grupo3		Henrique Santos CA	
Subject Name			
Country	PT		
State/Province/County	Braga		
Locality	Gulmaraes		
Organisation	UM		
Organisational Unit	EEUM		
Common Name	Grupo3		
Email Address	pg53793@alunos.uminho.pt		
Issuer Name			
Country	PT		
State/Province/County	Braga		
Organisation	Henrique Santos CA		
Organisational Unit	HS CA		
Common Name	Henrique Santos CA		
Email Address	hsantos@dsi.uminho.pt		
Validity			
Not Before	Fri, 22 Mar 2024 10:09:25 GMT		
Not After	Sat, 22 Mar 2025 10:09:25 GMT		
Public Key Info			
Algorithm	RSA		
Key Size	2048		
Exponent	65537		
Modulus	C0:4D:6E:01:32:92:52:B2:CF:80:7A:35:01:7F:7E:B9:38:85:13:6D:B5:6F:4D:9C:6		

Figura 37. Certificado público do recetor do e-mail.

Nota: Para o certificado do e-mail recetor fez-se o mesmo processo da criação do certificado explicada na secção 2.2.

Repara-se que a entidade certificadora do dois certificados é a mesma.

Passo 3: Deve-se editar as confianças do certificado da CA.

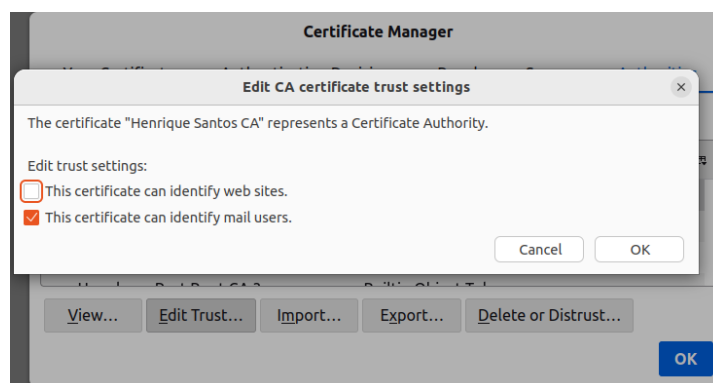


Figura 38. Confianças do CA.

Passo 4: O ficheiro do certificado deve ser escolhido como ficheiro para assinar e encriptar os e-mails.

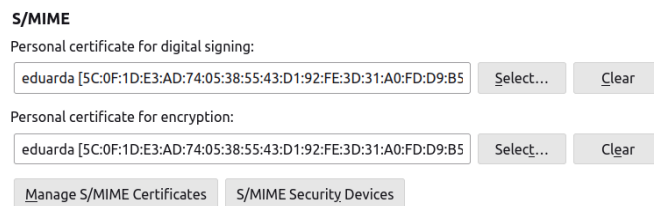


Figura 39. Encriptar e assinar.

Passo 5: Escrever e enviar a mensagem, sendo que está disponível a opção de encriptar e assinar o e-mail no S/MIME.

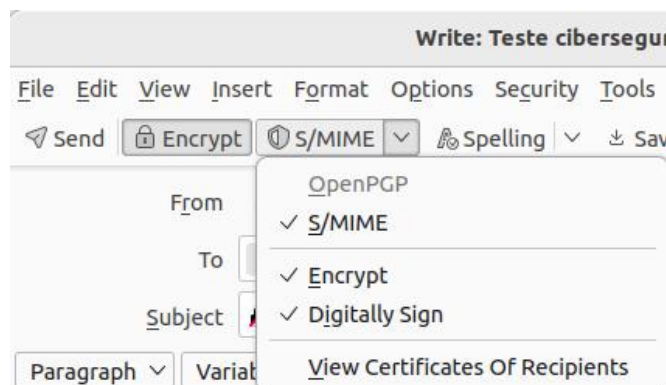


Figura 40. S/MIME.

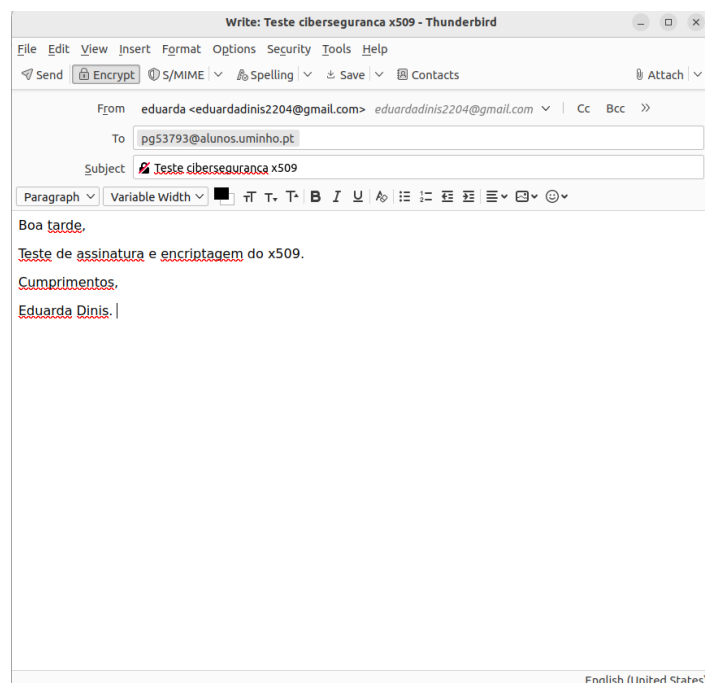


Figura 41. E-mail pronto a enviar.

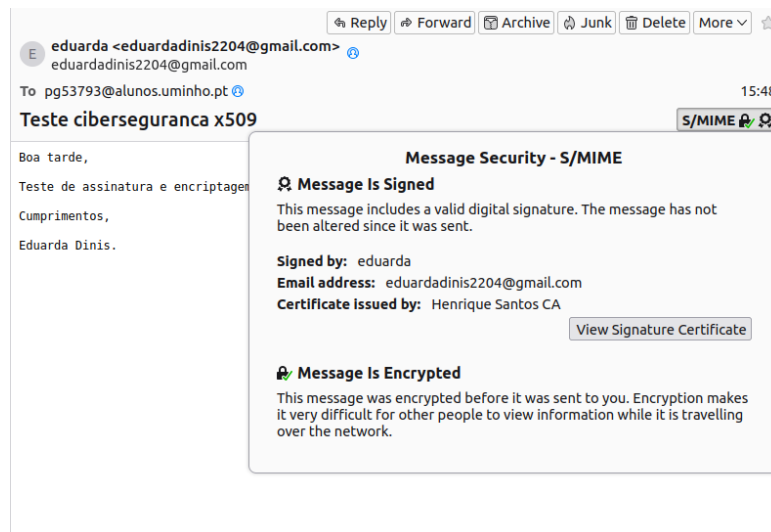


Figura 42. Envio da mensagem assinada e encriptada.

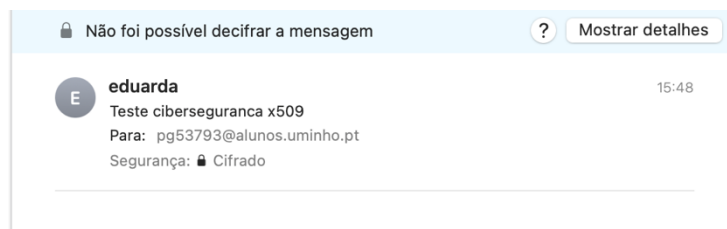


Figura 43. Receção da mensagem assinada e encriptada.

Observa-se que foi enviado o e-mail encriptado, e o e-mail recetor recebeu-o, mas sem conseguir observar nada.

4. Proteger Documentos Locais

Para experimentar as funcionalidades listadas no enunciando e utilizando a ferramenta *Kleopatra*, optámos por assinar /encriptar um ficheiro texto, mas o mesmo processo pode ser aplicado para por exemplo, uma pasta.

Passo 1: Seleção de assinar / encriptar o ficheiro no *Kleopatra*.

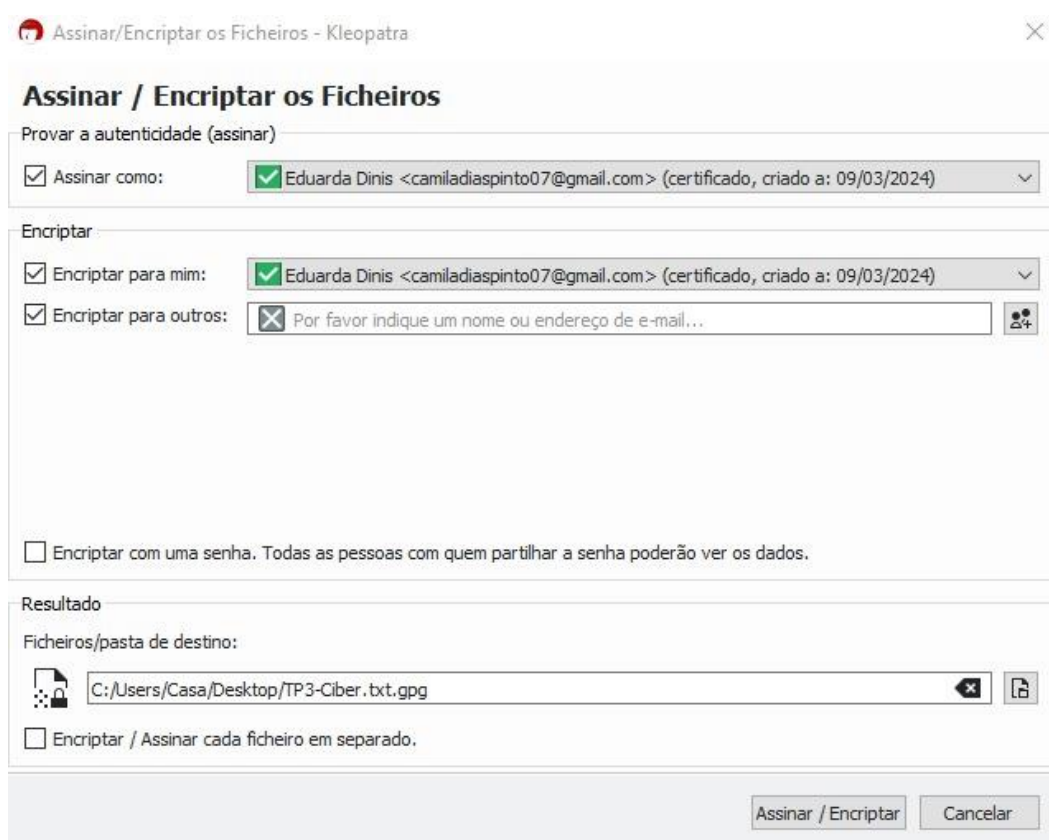


Figura 44. Encriptação do ficheiro.

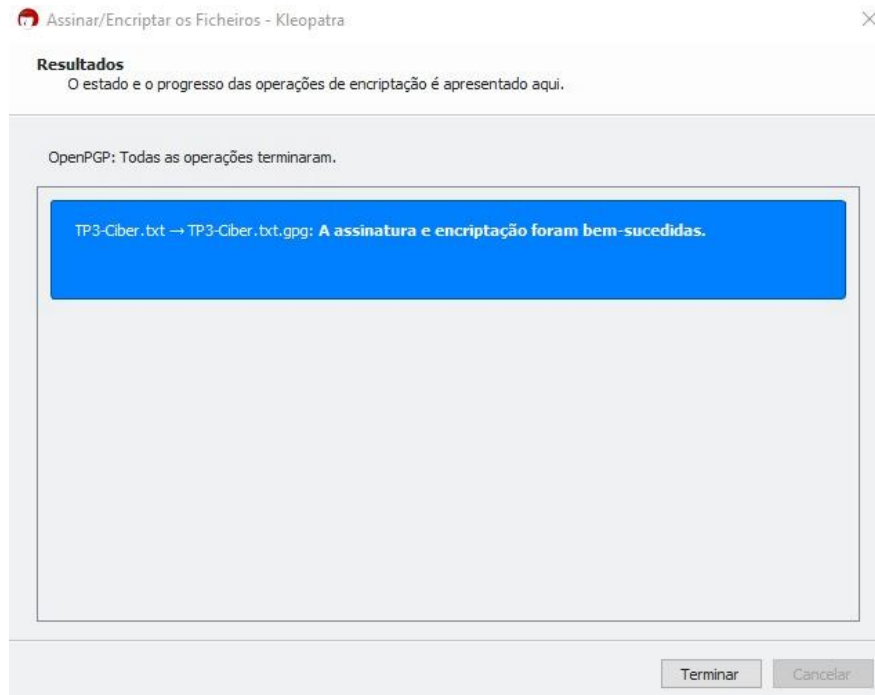


Figura 45. Sucesso na encriptação.

Passo 2: Testar a funcionalidade de decodificação do ficheiro.

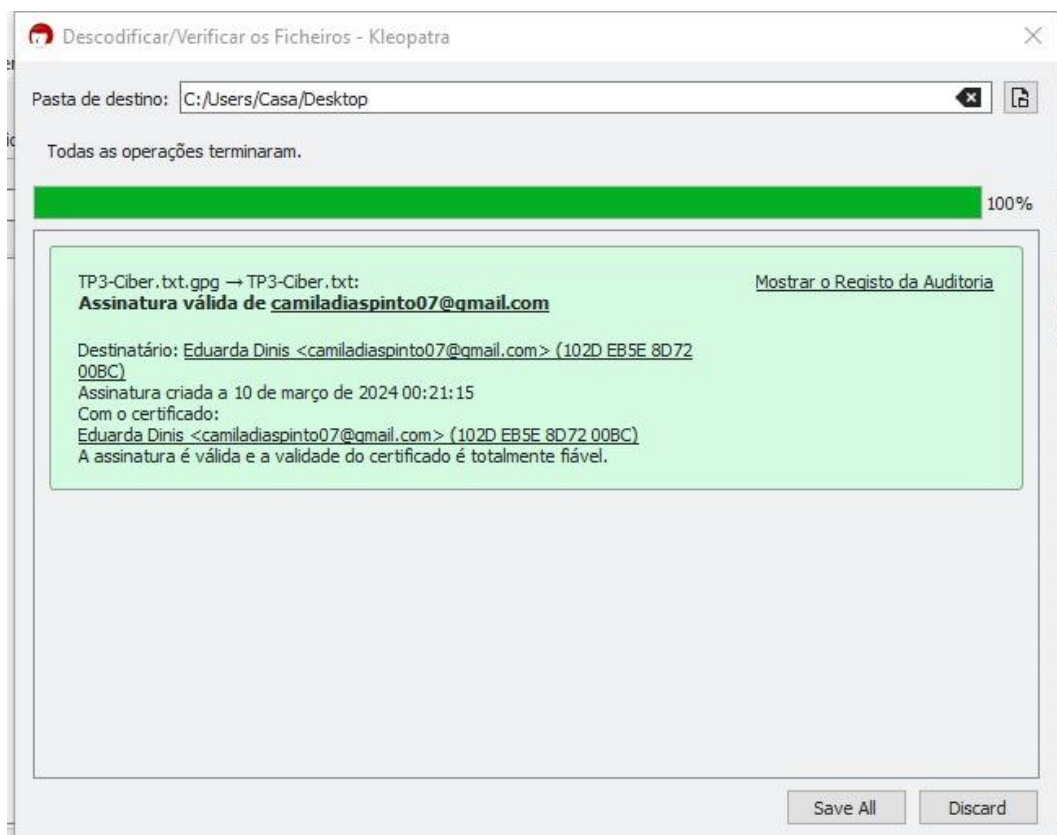


Figura 46. Sucesso na decifração.

Passo 3: Efetuar um teste onde a Camila encripta um ficheiro, mas desta vez usando a chave pública da Eduarda para que esta o possa decifrar.

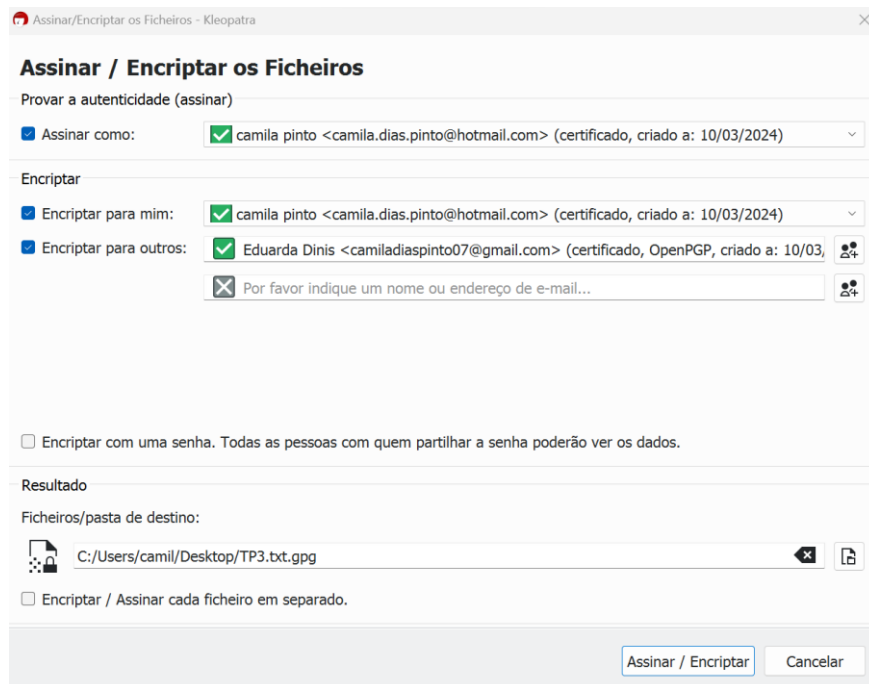


Figura 47. Encriptação do ficheiro.

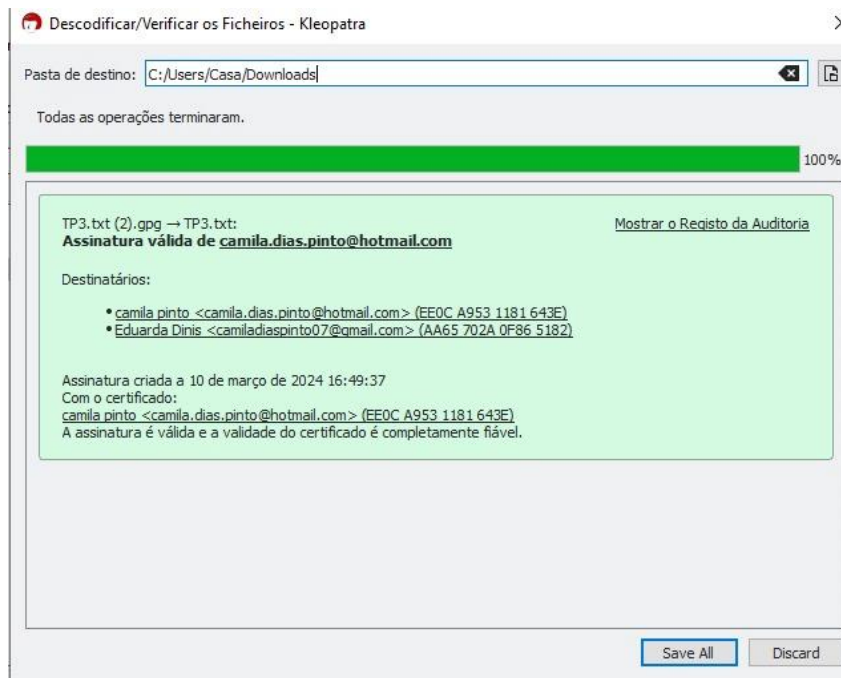


Figura 48. Sucesso na encriptação.

5. Tabela de Contribuição

Tarefa		Aluno	Tempo
Gestão de chaves	PGP	Camila Pinto	3 h
	X509	Eduarda Dinis	3 h
Enviar e receber mensagens seguras	PGP	Camila Pinto	3 h
	X509	Eduarda Dinis	3 h
Proteção documentos locais		Camila Pinto	2 h
Realização do logbook		Bárbara Fonseca, Bruno Santos, Gonçalo Dias	1 h

6. Conclusão

Em conclusão, ao comparar as implementações do PGP e do X509 para o envio e receção de mensagens encriptadas e assinadas, observa-se algumas diferenças e semelhanças.

O PGP oferece uma abordagem ponto a ponto para a segurança de comunicação, permitindo que os utilizadores criem e gerem as suas próprias chaves públicas e privadas. Isto proporciona um alto nível de controlo e independência aos utilizadores individuais.

Por outro lado, o X509 estabelece uma infraestrutura de chave pública mais centralizada, onde os certificados digitais são emitidos por autoridades certificadoras confiáveis. Isto proporciona uma abordagem mais escalável e amplamente aceite para autenticar identidades e garantir a segurança das comunicações em larga escala.