



Universidade do Minho  
Escola de Engenharia

---

**Universidade do Minho**  
**Trabalho Prático 3**  
**Certificados e PKIs**

---

1º Semestre – 2019/2020

Bruno Rodrigues Pg41066

Carlos Alves Pg41840

Paulo Bento a81139

## Índice

Introdução .....	3
Contextualização .....	4
Gestão de chave .....	5
Opção PGP .....	5
Alínea 2 .....	5
Alínea 4 .....	5
Alínea 6 .....	6
Alínea 7 .....	7
Alínea 9 .....	7
Alínea 10 .....	8
Alínea 11 .....	9
Opção X509 .....	10
Alínea 13 – Instalação OpenSSI .....	10
Alínea 14 .....	11
Alínea 15 .....	11
Alínea 16 .....	12
Alínea 17 .....	14
Alínea 18 .....	14
Enviar e receber mensagens seguras.....	17
Carlos Alves.....	17
Bruno Rodrigues .....	18
Paulo Bento .....	19
Alínea 2.....	20
Carlos Alves.....	20
Bruno Rodrigues.....	21
Paulo Bento.....	22
Alínea 3.....	22
Mensagem enviada de Carlos para Bruno.....	22
Mensagem enviada de Bruno para Carlos.....	23
Mensagem enviada de Paulo para Bruno.....	23
Alínea 4 – Revogação de certificados.....	24
Proteger documentos locais.....	26
Conclusão .....	27
Referências.....	28

## Introdução

Este trabalho prático, sugerido em aula na unidade curricular Segurança em Redes tem como objetivo descrever a forma como o conceito de chave pública é tipicamente implementado; reconhecer as operações associadas à geração das chaves públicas e privadas; aprender a usar as diversas ferramentas de gestão de certificados e ainda utilizar uma framework de criptografia para enviar e receber mensagens de e-mail e de modo que seja feito em segurança.

Assim sendo, foi nos requerido que escrevêssemos este documento, onde iremos colocar os resultados e respostas das questões presentes no enunciado.

## Contextualização

**Pretty Good Privacy** nada mais é que um software de criptografia que fornece privacidade criptográfica e autenticidade para comunicação de dados. É usado para criptografar, decryptografar e assinar textos, emails, arquivos, ou até mesmo partições de disco inteiras e ainda para aumentar a segurança do email.

Genericamente o PGP funciona da seguinte maneira

- A chave publica é usada para encriptar a mensagem;
- A chave privada desbloqueia ou descripta a mensagem encriptada;
- A chave publica é enviada para as pessoas/entidades que queremos receber mensagens ou então publica-la num site, para que elas possam criptografar mensagens confidenciais que desejam enviar para nós.
- Depois de receber a mensagem criptografada, usa-se a chave privada para decryptografá-la.

Conceitos importantes para o desenvolvimento deste trabalho:

**Encriptação:** processo de transformar informação usando uma cifra de modo a impossibilitar a leitura da informação a todos aqueles que não possuem uma identificação particular.

**Decryptação:** processo de tornar a informação encriptada novamente legível.

**Criptografia de chave privada:** Uso de apenas uma única chave, partilhada entre o recetor e o emissor. Tem a característica seguinte, a chave usada para cifrar é a mesma para decifrar. Muito Segura.

**Criptografia de Chave publica:** Uso de par de chaves (uma chave publica e outra privada), onde a chave publica é usada para a encriptação da mensagem e a privada para a descriptação.

**Certificado digital:** Documento eletrónico que tem como objetivo identificar virtualmente uma pessoa física ou jurídica (Wikipédia).

Inicialmente foram realizados os downloads e instalações dos programas sugeridos para abordar os temas deste trabalho prático. Foram instalados *OpenPGP*, e ainda juntamente com o *Kleopatra* o *GnuPG* e por fim o Thunderbird. *Kleopatra* usado como gestor de certificados.

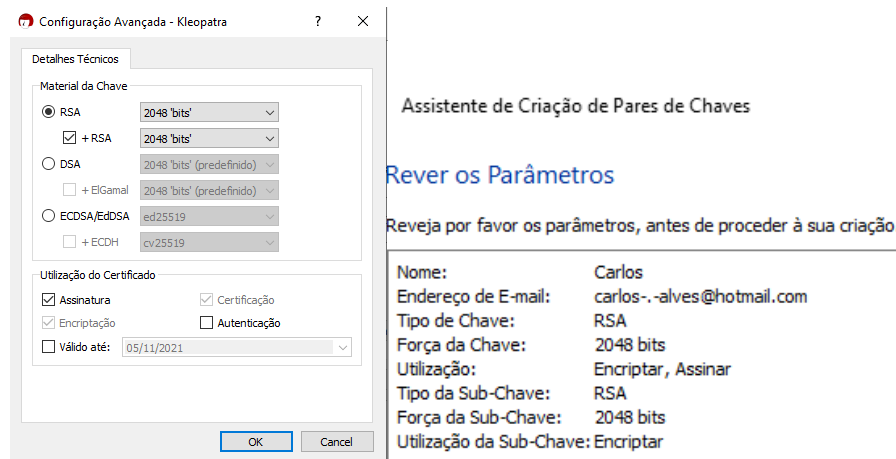
## Gestão de chave

### Opção PGP

#### Alínea 2

“Criar nova chave, escolha o tipo de chave RSA, com 1024/2048 bits. Não selecione nenhuma data limite de validade e mantenha para a cifra a lista de algoritmos, incluindo o AES, como predefinido”

Resposta: Nas imagens a baixo é possível observar a criação e configuração do par de chaves nos requisitos pretendidos.



### Par de Chaves Criado com Sucesso

O seu novo par de chaves foi criado com sucesso. Veja abaixo por favor os detalhes do resultado, assim como alguns passos seguintes sugeridos.

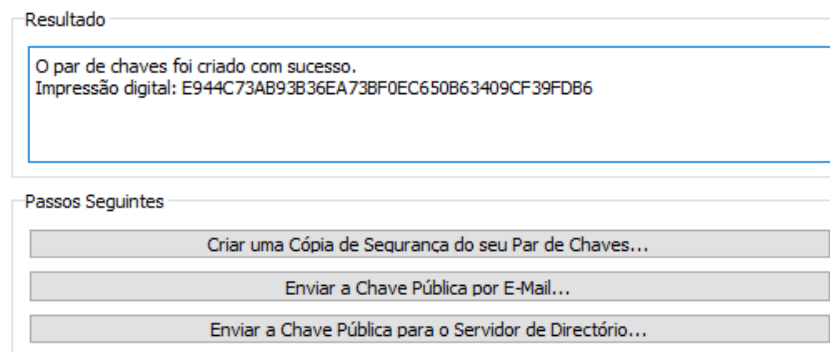


Figura 1. Criação nova chave

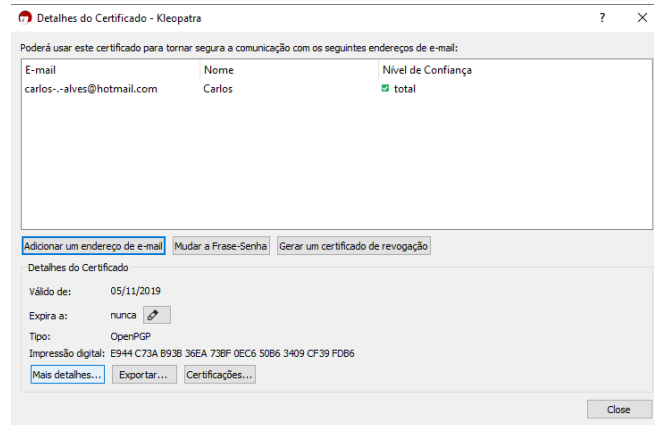
#### Alínea 4

Foi nos solicitado uma *Passphrase*, então colocamos uma sequência de fácil memorização para depois conseguirmos utilizar a chave privada (assinatura/decifrar) que geramos anteriormente.

## Alínea 6

“Copie os atributos mais relevantes da assinatura e da chave e da *fingerprint* (...) Esta chave é a sua chave privada ou a pública? Que elementos ligam a assinatura com a sua chave privada?”

A chave exibida nos prints abaixo é a chave pública. Representação hexadecimal da *fingerprint* e da chave publica. A ligação da assinatura com a sua chave privada deve-se ao fato de ser calculado o *hash* da mensagem, de seguida esse *hash* é criptografado com a chave privada para criar a assinatura.




```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Comment: ID do Utilizador: Carlos <carlos-.alves@hotmail.com>
Comment: Criada: 05/11/2019 18:27
Comment: Tipo: 2048-bit RSA (chave privada disponível)
Comment: Utilização: Assinatura, Encriptação, ID's de Utilizador de
Certificação
Comment: Impressão Digital: E944C73AB93B36EA73BF0EC650B63409CF39FDB6

mQENBF3Bv4BCAC7yPMibKQmQg3B1wGJBHmkZt8MxNyn/bAeHfVsOgN3ZQdF9Ccc
By6mMcp7YnQGPkyOGaWseTa2vqccC2vIps046EdInRNbklHie20P1kINoiMAejf
BVeC14NhRV3cl4grX3B9WOqjaI33WB9SbPp7S+JaUoYBsiqs5zylbmd/R2Sryt
KPCqseP3xCGCGUDm4FhRgA+UshVgoL0xhd/Pk012kSGEiljAvlfe2S2S9XCedfei
2P2Plsyj6H94mcS02jqlVJfIWeV94zrf3kDcoJx3zNo5erQb104LnJ7xMlytbHUv
045UkIa/sruluKjuHj2CTIQf2GfJ2iafT0tABEBAAQI0NhmcmvvcyA8Y2FybG9s
LS4tYWx2ZXNNAaG90bWp0C5jb20+QFOBBMBCAA4FiEE6UTHork7Nuprvv7GULY0
C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85
/bAeQqAgbFS41acTU99qv6F/AEoue8OtIPTnnJcti7s1X2/pIaGedGQyWsgaV6HhP
BnSFQcY3bZa3sxqatCnN9o6RTj1E7T41Og69/kcRsK+fmD19oRcJaiU5jR0U13gSe
cs6ppQxg8G3v05Wd+sgRRRKt8pvcSpsTco10rUYPNI7A2BuiqAzJ50bApCZPpDac
htmCwQqJgUgU610KV5V+1yTNMyCJy5CU+aAuOPU00L/qj1A40cL7RuAnIvW30qI
Jm5FtLalDjqlUOp+I/C03Apsh6ob2lpJDIB5Xg8up5nM9TaLVu4MatvGvW30qI
1hwHase3+ErKL2oug27jgy9lCFZT57kBDQRdwb7+AqgAwgKD3jlcxsD/54K59s4Z
drymv620jcs94cYvUSglZxdNerEQNIhlxOv8Bym0B7gyo26u0JzRqB999j8ms0IuHi
ay4ummjgSn3tIDm8eAJVp322zAV18vsnhneCokI18F7yvfHfnKerUgaYVKe3UGCI
xj6d+wyTz16kHqAc06TuQAxmf57x12xkh0nhkLdtxiSoomuYxiXvu3BB2CtVf0
6hBj9+wkRQ6whN1aHqolzgI7LrOxHLNQQDW3juzNc+rvjoEoXlkuB8evf2Vp90c
Trh+1SVh08u4GTaHEWfObfyjQ9H0VM2K5LyL5STucx1CL4vEN9QDchAo2CORRD0
1wARAQAABiQE2BBgCAAAgFiEE6UTHork7Nuprvv7GULY0C85/bYfA13Bvv4C6wA
CgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQ
ULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0
C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/
bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA
13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv
4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6w
AFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwk
IBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIG
FQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJ
CAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAas
CBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBC
VCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAw
ECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHg
ECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4
AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgk
QULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0
C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/
bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA
13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv
4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6w
AFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwk
IBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIG
FQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJ
CAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAas
CBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBC
VCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAw
ECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHg
ECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4
AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgk
QULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0
C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/
bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA
13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv
4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6w
AFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwk
IBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIG
FQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJ
CAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAas
CBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBC
VCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAw
ECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHg
ECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4
AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgk
QULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0
C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/
bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA
13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv
4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6w
AFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwk
IBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIG
FQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJ
CAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAas
CBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBC
VCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAw
ECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHg
ECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4
AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgk
QULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0
C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/
bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA
13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv
4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6w
AFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwk
IBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIG
FQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJ
CAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAas
CBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBC
VCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAw
ECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHg
ECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4
AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgk
QULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0
C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/
bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA
13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv
4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6w
AFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwk
IBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIG
FQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJ
CAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAas
CBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBC
VCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAw
ECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHg
ECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4
AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgk
QULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0
C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/
bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA
13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv
4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6w
AFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwk
IBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIG
FQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJ
CAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAas
CBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBC
VCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAw
ECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHg
ECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4
AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgk
QULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0
C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/
bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA
13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv
4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6w
AFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwk
IBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIG
FQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJ
CAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAas
CBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBC
VCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAw
ECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHg
ECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4
AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgk
QULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0
C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/
bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA
13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv
4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6w
AFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwk
IBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIG
FQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJ
CAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAas
CBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBC
VCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAw
ECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHg
ECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4
AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgk
QULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0
C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/
bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA
13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv
4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6w
AFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwk
IBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIG
FQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJ
CAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAas
CBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBC
VCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAw
ECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHg
ECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4
AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgk
QULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0
C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/
bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA
13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv
4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6w
AFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwk
IBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIG
FQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJ
CAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAas
CBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBC
VCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAw
ECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHg
ECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4
AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgk
QULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0
C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/
bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA
13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv
4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6w
AFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwk
IBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIG
FQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJ
CAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAas
CBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBC
VCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAw
ECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHg
ECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4
AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgk
QULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0
C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/
bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA
13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv
4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6w
AFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwk
IBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIG
FQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJ
CAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAas
CBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBC
VCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAw
ECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHg
ECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4
AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgk
QULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0
C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/
bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA
13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv
4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6w
AFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwk
IBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIG
FQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJ
CAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAas
CBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBC
VCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAw
ECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHg
ECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4
AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgk
QULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0
C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/
bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA
13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv
4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6w
AFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwk
IBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIG
FQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJ
CAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAas
CBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBC
VCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAw
ECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHg
ECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4
AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgk
QULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0
C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/
bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA
13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv
4C6wAFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6w
AFcwkIBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwk
IBwIGFQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIG
FQoJCAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJ
CAasCBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAas
CBBCVCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBC
VCAwECHgECF4AACgkQULY0C85/bYfA13Bvv4C6wAFcwkIBwIGFQoJCAasCBBCVCAw
ECHgECF4AACgkQ
```

## Alínea 7

“Essas subchaves são chaves publicas ou privadas? Qual é a relação destas com a chave master? Qual a utilidade de ter várias subchaves associadas a uma mesma chave?”

Em relação á geração de outras sub-chaves, o *Kleopatra* não nos permitiu gerar mais que as exibidas na imagem abaixo, relativas à chave master gerada nas alíneas anteriores.

 Detalhes das sub-chaves - Kleopatra

Sub-chaves:							
ID	Tipo	Válida De	Válida Até	Estado	Força	Utilização	Primária
50B6 3409 CF39 FDB6	RSA	05/11/2019		boa	2048	Certificar, Assinar	✓
7C8D 32B7 DA4D E990	RSA	05/11/2019		boa	2048	Encriptar	

Figura 3. Detalhes das sub-chaves

## Alínea 9

Configuração da aplicação para o servidor PGP, como é possível concluir com a figura abaixo, o PGP já vem configurado para utilizar um repositório global suportado pela organização que fornece o *OpenPGP*. Aqui foi adicionado um novo servidor, que utilizará o protocolo PGP *Keyserver* HTTP, o nome do servidor é pgpkeys.mit.edu e a porta 11371.

## Servidor PGP

**Configuração dos serviços de directório**

Servidor de Chaves do OpenPGP:

Serviços de directório X.509:

Nome do Servidor	Porto do Servidor	DN de base
pgpkeys.mit.edu	11371	

Figura 4. Configuração dos serviços de diretório.

Alínea 10

Questão: “Utilizando o site web referido no passo 8, procure por chaves publicas através de um endereço de email e depois por nome. Comente o resultado obtido.”

## 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 UM) &lt;hsantos@dsi.uminho.pt&gt;</a>
pub	1024D/ <a href="#">475D4617</a>	2006-07-13	<a href="#">Henrique M D Santos (No) &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="#">319D3D84</a>	2001-06-15	<a href="#">Henrique Manuel Dinis dos Santos &lt;hsantos@dsi.uminho.pt&gt;</a>

Figura 5. Resultados da procura no site por email

## Search results for 'santos henrique'

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="#">86E90D2B</a>	2018-10-23	<a href="#">Henrique Santos &lt;henrique.santos@inf.aedb.br&gt;</a>
pub	3072R/ <a href="#">F3C5E85D</a>	2018-08-29	<a href="#">Henrique dos Santos Goulart &lt;henrique.goulart@chaordicsystems.com&gt;</a>
pub	1024D/ <a href="#">E759B578</a>	2018-06-12	<a href="#">Luiz Henrique Silva Santos &lt;luizhenriqueeduardoss@gmail.com&gt;</a>
pub	2048R/ <a href="#">37F1E1F6</a>	2018-05-16	<a href="#">Carlos Henrique dos Santos &lt;kc-ny@hotmail.com&gt;</a>
pub	4096R/ <a href="#">5EC3299C</a>	2018-02-17	<a href="#">Launchpad PPA for Matheus Henrique dos Santos</a>
pub	2048R/ <a href="#">6B54B960</a>	2018-02-17	<a href="#">Matheus Henrique dos Santos &lt;vorj.dux@gmail.com&gt;</a>
pub	4096R/ <a href="#">B4A4A88A</a>	2016-10-26	<a href="#">Pedro Henrique Oliveira dos Santos (RELEASE SIGNING KEY) &lt;pedro@apache.org&gt;</a>
pub	2048R/ <a href="#">3473AE1C</a>	2016-09-14	<a href="#">Henrique Santos (Chave para uso na UM) &lt;hsantos@dsi.uminho.pt&gt;</a>
pub	4096R/ <a href="#">618AD012</a>	2016-05-20	<a href="#">Renan Henrique Santos da Silva &lt;renanh2008@hotmail.com&gt;</a>
pub	1024R/ <a href="#">7B4DCD73</a>	2014-04-27	<a href="#">Rafael Henrique Santos Oliveira &lt;rafael_ptc@hotmail.com&gt;</a>
pub	1024D/ <a href="#">4350FE61</a>	2014-03-14	<a href="#">Jorge Branco (Prof Henrique Santos) &lt;jorgebranco@iol.pt&gt;</a>
pub	4096R/ <a href="#">D3490EC5</a>	2011-04-15	<a href="#">Michel Henrique Aquino Santos (Chave Michel) &lt;michel.has@gmail.com&gt;</a>



pub	2048R/99AA2678	2010-07-24	<a href="#">Paulo Henrique Andrade Domingues Rodrigues Santos (OAB/RJ 155991) &lt;phadrs@gmail.com&gt;</a>
pub	1024R/CA6436DF	2010-03-18	<a href="#">Henrique M. D. Santos &lt;henrique.dinis.santos@gmail.com&gt;</a>
pub	1024D/475D4617	2006-07-13	<a href="#">Henrique M D Santos (No) &lt;hsantos@dsi.uminho.pt&gt;</a>
pub	1024D/378C4FA3	2005-06-15	<a href="#">Henrique Gamboa dos Santos (IT Student) &lt;themage@internet.lu&gt;</a>
pub	1024D/F617B540	2004-10-19	<a href="#">Fabio Henrique Silva dos Santos (FZ-Juelich, ICG-I) &lt;f.h.silva.dos.santos@fz-juelich.de&gt;</a>
pub	1024D/847E883F	2004-09-29	<a href="#">Flavio Henrique Reis Santos &lt;fhrrs@npd.ufal.br&gt;</a>
pub	1024D/3AE27210	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/48A06015	2003-06-11	<a href="#">Luis Henrique dos Santos Velho &lt;activate@databrum.com.br&gt;</a>
pub	1024D/19ACB10D	2002-06-16	<a href="#">Jose Henrique Bessa dos Santos &lt;hbessa@iis.com.br&gt;</a>
pub	1024D/915244F0	2002-02-26	<a href="#">Henrique M D Santos &lt;santos.henrique@clix.pt&gt;</a>
pub	1024D/319D3084	2001-06-15	<a href="#">Henrique Manuel Dinis dos Santos &lt;hsantos@dsi.uminho.pt&gt;</a>
pub	1024D/32245D84	2001-06-12	<a href="#">Henrique Carvalho Santos &lt;henrique.carvalho@tjdf.gov.br&gt;</a>
pub	1024D/AC533CE9	2000-03-31	<a href="#">Claudio Henrique Fontenelle Santos &lt;csantos@inova.net&gt;</a>
pub	1024D/4838B581	1999-10-31	<a href="#">Paulo Henrique Andrade Domingues Rodrigues Santos &lt;pauloh@newview.com.br&gt;</a>
pub	1024D/3F914880	1999-05-16	<a href="#">haroldo henrique santos &lt;haroldo henrique@uol.com.br&gt;</a>

Figura 6. Resultados da procura no site por nome

Ao seguir as instruções do enunciado deparamo-nos que aquela funcionalidade não se encontrava no software, então acedemos ao web site diretamente e realizamos a busca pelo nome “Henrique Santos” e pelo respetivo email.

Como é possível observar, a relação dos resultados de chaves públicas entre o nome e um email é notória. Como é mais provável que existam nomes iguais ou semelhantes ao inserido, o resultado obtido é muito mais alargado do que se for inserido um email. Tais conclusões podem ser observadas nas figuras acima.

#### Alínea 11

Questão: “Faça o envio por email de uma chave com o colega e descreva o processo usado. Após a receção deverá fazer mais alguma operação, antes de utilizar a chave do seu colega?”

*\*Kleopatra não permite o envio da chave por email – mozilla Thunderbird\**

Visto que o *Kleopatra* não nos permite o envio da chave por email, instalamos o Mozilla Thunderbird em conjunto com a extensão *Enigmail* que nos permite ter acesso às chaves que temos no *Kleopatra* e envia-la por email.

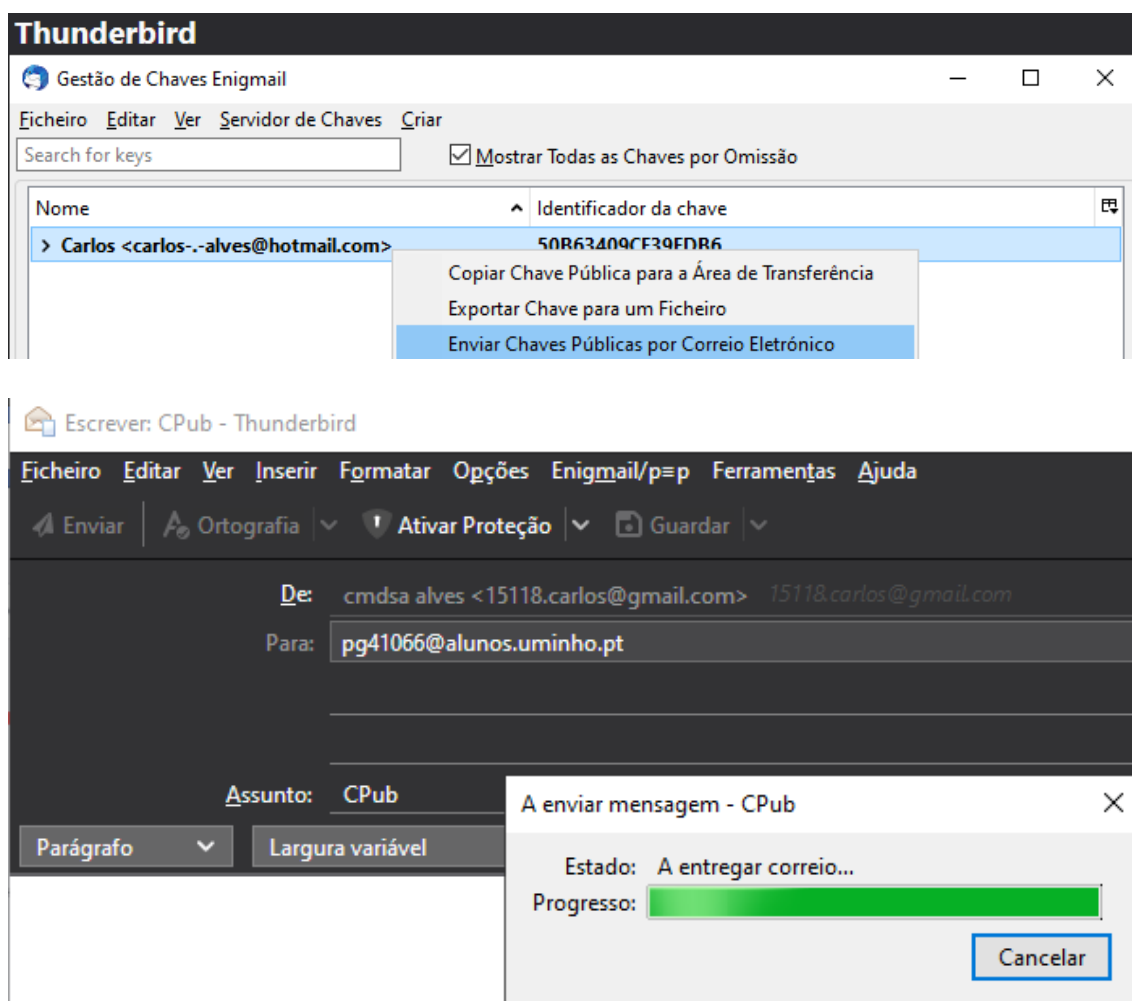


Figura 7. Envio da chave para um colega, usando Thunderbird com o *addon Enigmail*.

### Opção X509

#### Alínea 13 – Instalação OpenSSL

Depois de instalado o *OpenSSL*, geramos um par de chaves que irá criar uma chave privada e a chave publica associada de tamanho 2048. Através do comando:

- `genrsa -out privkey.pem 2048`

```
C:\Program Files\OpenSSL-Win64\bin>openssl.exe
OpenSSL> genrsa -out privkey.pem 2048
Generating RSA private key, 2048 bit long modulus (2 primes)
.....+++++
.....+++++
e is 65537 (0x010001)
OpenSSL>
```

Figura 8. Geração da chave

## Alínea 14

Verificação do estado da chave e com a nova chave privada. Como é possível observar o estado encontra-se em bom estado - cifra/assinatura.

```
OpenSSL> rsa -in privkey.pem -check
RSA key ok
writing RSA key
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAPlxn2p47s5EbvL20cUAKF0Avn45qjcGQdsmCB+4eghtbP6D
103TVxLjVDOh1KJIbSILOFK3YtVh3YlMbTXYrPHgHtQRy0/Tg4BwYwmmBtJnZj
HSZXpP668iJEyrnp679AmGo9dQYRLZPWSDOe8NPAPHiNNwEm5f1NobxuKCdzBKGU
w+p0oj4jUzy0CTr/hGvND/FQJpJiWTrs2B0a4/GQNMylTmR1iV8BED2+0ly53X3J
UoCXSm3LX8v05EiMR00p1HAB9vELS8KJ2oFrkIJU0G4Vv2X20aX+l4mxSdGpWlvj
RBM/U9JqyLwStFvSqJXzI9+jJAXdd6l1HgRm3QIDAQABaoIBABv6docatXlt2RXw
JOJit2ZCdsS9X5FDUkc0CGtyJtQuhrEB/Kzj3G52yxxRIAEeUMNgknBfWNFomqw
YawrZmMBGQ0VtMoE+fVtf2epp2F920sxhfUf4yJiAhdfWZgGNIRx0vd960FzN4He
/H/OHL8dLpd7ZbT6F68/dIn4ovqQs1VMRG05e4hIUQ6IgdQoPx0wHd+WwJ6PjC
dqPP6dSPtES4dvveDlw1zfzy7A2yBVTQFb1eX2AMPdMZT8FfvhRJcOP05r3sj4DK
JSYHJwHbZyE7mxVQJFMJLvksoS1iQ6PFGVh/2r7FEI9AoJhmEFvYw8jWh5Vqg93A
noiYAmECgYEA8DMHyuK/K1mjYoXbojIyHYy5/NJvyxAbj7jtiv4/jjdVAHRXJleH
kbrqTXxhRmeBvm3kjXRPYCiak7Vfd9wGLKA0t4RLYd08uF1UadmestQ5rC132s5T
uBhlqWiQ61bUxzR4BR0fTToXoGICnfCq7+btgIG/eZyYkLuPwv4VSckCgYEAYwFI
Vn04+coDslWqkVBNf5t25Qip/gB2363l97qc1w1+fR0f8huWd09jXLqzQldUX1Qf
TPqaUugz4+eNDLmMQ46+KyY2WgcQDdWwUMXmpneg5AhhHLR40ze3xu3A5BpHDq
lHkvbyssmctYtiRsFXEUSYnD6f+uRmwKLLiTPnUCGYAou960b20QDHGcwcSPawFI
rxBTYzSGMUMbSncuPR02IHgPzasB25IoCpS1c0Rj1iXQj35U5sao4Qnlxrbp7z6d
ksWd4ZePDYNRMli6CSe6l/b31fYfayITdD+5TPxwYUdQSPuZkmi+hF1/u19KPYgf
iv/37Qj1rLLKyKQGo2Qk0KBgQCH7cJZDpsuAriB+K04i7DySbNyrsmWgyu3hP8r
Ncg6nU7AFBMBGblYdafgOknb/dD8eY4EIjC3xfIPg8drRUKBnpUoJoTs7p7dB9e1
WZTDcvOpaXIImPSrUFK001t7Nyf4WrkHYc6wwbvFRGdn7qb/xaTCiPcvi39MSgiH
7D58LQKBgQDgCKyunSI/p8UPeo41sYAAMQGwdy0yecqkCfLAdycv/qWhdZvQi09Z
hWAHrHHMfEmI6N6f2d0xCeGVnGECshIgkibL3owxJzo1qWYAXZWkt4xDm1hTst1x
ghCDVNC6lZ6qToJZiW+pvv7ny0c2hvy6ZcFYjt9mm00dJ2XGoNS4Aw==
-----END RSA PRIVATE KEY-----
OpenSSL>
```

Figura 9. Verificação da chave gerada

## Alínea 15

Gerar pedido de certificado, aqui inserimos algumas informações como *Common Name*, endereço de email, cidade, País entre outros. Estas informações são incluídos no certificado.

```
calvare@calvare-X541UV:~$ 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) []:Braga
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Uminho
Organizational Unit Name (eg, section) []:Uminho
Common Name (e.g. server FQDN or YOUR name) []:Carlos Alves
Email Address []:pg41840@alunos.uminho.pt

Please enter the following 'extra' attributes
to be sent with your certificate request
```

Figura 10. Geração de pedido de certificado

```

verify OK
Certificate Request:
Data:
  Version: 1 (0x0)
  Subject: C = PT, ST = Braga, L = Braga, O = UMinho, OU = Uminho, CN = Carlos Alves, emailAddress = pg41840@alunos.uminho.pt
  Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public-Key: (2048 bit)
    Modulus:
      00:9c:7d:75:96:ba:c2:fe:6d:0c:d5:6c:33:e6:dc:
      d3:41:f2:2a:62:9f:c3:73:d3:03:86:1d:3f:37:db:
      88:f0:f2:ab:c3:56:9f:35:90:4d:ea:37:18:69:d8:
      07:32:4a:27:c8:e7:62:af:fd:38:a5:f2:ba:10:9d:
      83:0d:0d:a6:66:76:a1:f3:4f:53:4c:e2:12:73:ef:
      1f:d5:8a:98:c1:e8:61:db:80:79:14:ba:4d:db:16:
      b3:5c:e8:0a:65:81:dd:ac:1e:a5:9c:2d:c1:58:64:
      a4:db:85:b4:9e:68:b9:04:09:2e:86:ad:b6:a8:f7:
      14:6c:af:9f:9e:e7:6b:6d:e1:1f:59:46:9d:19:a8:
      5b:39:2c:1b:1f:ba:53:2d:9e:73:d6:45:9d:5c:ff:
      b5:98:f2:2c:32:16:ac:ce:48:53:2b:3f:b3:83:b5:
      22:f7:03:12:50:c7:6f:33:05:0e:1f:81:df:12:24:
      06:ac:af:eb:28:ee:45:07:48:95:22:b4:1a:ca:1f:
      24:55:fb:4b:da:0c:e3:01:5a:0f:08:e1:74:b5:06:
      6a:95:06:6d:aa:60:e3:c4:d9:8d:f5:f7:cc:83:24:
      34:5e:dc:31:ac:ae:1f:f3:97:dd:b0:ac:dd:d7:6e:
      7b:74:e0:30:d9:08:16:65:8c:15:5b:81:47:12:d0:
      05:ed
    Exponent: 65537 (0x10001)

Signature Algorithm: sha256WithRSAEncryption
40:61:e4:0e:9e:56:ad:67:4d:55:f5:3c:12:c1:f5:93:d6:01:
c5:cf:4b:c6:3d:6f:e0:67:5f:0d:42:c6:47:2b:35:33:a8:4d:
c2:8c:55:c3:28:33:e4:92:4b:64:a8:3a:d8:fe:28:7b:ed:b5:
52:af:7a:5f:54:a4:b9:b4:57:96:fd:c5:8a:2f:53:8d:71:e4:
08:24:90:79:7e:75:6a:08:ce:66:48:cd:8c:3d:90:cd:ac:db:
69:4b:a5:fc:52:d2:4a:c0:52:8f:b4:55:cb:2e:b8:f6:02:40:
c6:c9:11:8e:f6:79:07:0f:5b:cc:d6:25:82:2f:72:dc:1f:fe:
1f:8f:e0:69:c4:5a:a1:0d:23:4d:11:71:46:96:d4:9c:77:64:
71:ea:95:aa:c2:2d:00:52:eb:d4:95:f6:0e:f3:8b:7e:ab:5d:
f6:25:cb:df:d6:41:2f:f0:7b:34:a0:0b:b3:1c:3d:f5:72:e0:
f9:32:a4:e3:5e:77:c7:23:a5:22:70:28:3e:58:94:4f:16:7e:
36:c0:93:bd:10:da:a2:d1:8f:6d:f9:d6:98:cd:43:6e:5f:de:
36:e0:dc:65:10:63:86:e2:dc:80:73:5e:46:95:3b:1e:75:6d:
04:a0:06:de:76:83:1e:c7:1f:08:09:b1:84:9e:8d:bd:fb:c5:
d4:c5:0f:2a

```

Figura 11. Verificação do estado do nosso ficheiro com o certificado.

## Alínea 16

Abaixo temos a geração do certificado auto assinado, que é gerado usando a chave privada e o CRS (passo realizado anteriormente) usamos o comando:

```

Signature ok
subject=C = PT, ST = Braga, L = Braga, O = UMinho, OU = Uminho, CN = Carlos Alves, emailAddress = pg41840@alunos.uminho.pt
Getting Private key

```

Figura 12. Geração do certificado auto assinado

De seguida, temos a verificação do ficheiro com o certificado auto assinado.

Elementos relevantes temos: o certificado, a assinatura digital e a chave pública. Além disso temos o *Serial number* que é atribuído pela CA ao certificado, este *serial number* em princípio é único e exclusivo deste certificado emitido. Basicamente o nome do emissor e o *serial number* são necessários para identificar um certificado único.

```
calvareze@calvareze-X541UV:~$ openssl x509 -text -in privcert.crt
Certificate:
    Data:
        Version: 1 (0x0)
        Serial Number:
            45:26:9a:2e:e6:a0:37:08:e6:39:ec:ae:cc:57:00:2d:c8:dc:04:f4
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = PT, ST = Braga, L = Braga, O = UMinho, OU = Uminho, CN = Carlos Alves, emailAddress = pg41840@alunos.uminho.pt
        Validity
            Not Before: Nov  8 20:04:11 2019 GMT
            Not After : Dec  8 20:04:11 2019 GMT
        Subject: C = PT, ST = Braga, L = Braga, O = UMinho, OU = Uminho, CN = Carlos Alves, emailAddress = pg41840@alunos.uminho.pt
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:9c:7d:75:96:ba:c2:fe:6d:0c:d5:6c:33:e6:dc:
                    d3:41:f2:2a:62:9f:c3:73:d3:03:86:1d:3f:37:db:
                    88:f0:f2:ab:c3:56:9f:35:90:4d:ea:37:18:69:d8:
                    07:32:4a:27:c8:e7:62:af:fd:38:a5:f2:ba:10:9d:
                    83:0d:0d:a6:b6:76:a1:f3:4f:53:4c:e2:12:73:ef:
                    1f:d5:8a:90:c1:e8:61:db:00:79:14:ba:4d:db:16:
                    b3:5c:e8:0a:65:81:dd:ac:1e:a5:9c:2d:c1:58:64:
                    a4:db:85:b4:9e:68:b9:04:09:2e:86:ad:b6:a8:f7:
                    14:6c:af:9f:9e:e7:6b:6d:e1:1f:59:46:9d:19:a8:
                    5b:39:2c:1b:1f:ba:53:2d:9e:73:d6:45:9d:5c:ff:
                    b5:98:f2:c2:32:16:ac:ce:48:53:2b:3f:b3:83:b5:
                    22:f7:03:12:50:c7:6f:33:05:0e:1f:81:df:12:24:
                    06:ac:af:eb:28:ee:45:07:48:95:22:b4:1a:ca:1f:
                    24:55:fb:4a:da:0c:e3:91:5a:0f:08:e1:74:b5:06:
                    6a:95:06:6d:a6:60:e3:c4:e9:0d:15:f7:ce:83:24:
                    34:5e:dc:31:ac:ae:1f:f3:97:dd:b0:ac:dd:d7:6e:
                    7b:74:e0:30:d9:08:16:65:8c:15:5b:81:47:12:d0:
                    05:ed
                Exponent: 65537 (0x10001)
```

```
Signature Algorithm: sha256WithRSAEncryption
    80:50:76:c7:66:16:5c:b2:2f:1f:66:b2:7d:b0:0d:63:b1:53:
    df:11:d9:19:86:e5:7a:f4:94:68:4c:83:36:82:3f:f3:00:f8:
    60:69:0b:6c:9c:f4:80:69:b6:fa:ff:4b:b3:32:fe:ad:10:94:
    03:68:06:17:6b:b1:cb:20:0f:4f:a5:b8:90:68:aa:8b:36:ce:
    0e:55:21:de:d2:25:42:11:7e:d3:d2:e4:4f:ef:2a:a6:f7:22:
    c4:01:d4:4b:ca:0d:4a:0a:cb:33:4d:30:72:0a:3e:b8:cb:46:
    a5:9e:29:cc:63:78:cd:95:2a:71:f5:12:13:b0:79:6a:92:79:
    2f:cd:4a:8a:43:e0:39:e1:9e:79:37:9a:19:cc:b3:28:72:5a:
    fb:f6:23:11:d1:1f:1d:3b:a0:aa:f2:c5:c4:5e:40:ac:c7:0e:
    89:6f:90:32:0b:38:9a:6f:bb:35:f9:af:f6:ea:63:ac:93:b0:
    a3:3e:e8:3a:f5:94:b1:7d:a9:41:94:b6:fe:42:28:22:d1:e3:
    a0:78:ce:3d:81:b8:c4:f2:2d:dc:40:44:17:4d:98:47:a9:1a:
    6e:59:94:cd:18:76:0f:0a:07:ce:ce:e7:82:cb:9c:6f:04:6e:
    98:8c:82:8c:c4:a8:b1:4d:6b:eb:16:82:55:70:1f:7b:dc:39:
    10:89:9b:06
-----BEGIN CERTIFICATE-----
MIIDPzCCAo8CFEUmmi7moDcI5jnsrsxXAC3I3AT0MA0GCSqGSIb3DQEB
CwUAMIGP
MQswCQYDVQQGEwJQVDE0MAwGA1UECAwFQnJhZ2ExDjAMBGNVBAcMBUJy
YWdhMQ8w
DQYDVQQKDAZVTWluaG8xZDZANBgNVBASMB1VtaW5obzEVMBMGA1UEAwM
Q2FybG9z
IEFsdmVzMScwJQYJKoZIhvcNAQkBFhhwZzQxODQwQGFsdW5vcy51bW
luaG8ucHQw
HhcNMTkxMjA4MjAwNDEwNjAwNDEwNjAwNDEwNjAwNDEwNjAwNDEwNj
AwNDEwNj
DjAMBGNVBAcMBUJyYWdhMQ4wDAYDVQQHDAVCcmFnYTEPMA0GA1UECgw
GVU1pbmhv
MQ8wDQYDVQQQLDAZVbWluaG8xFTATBgNVBAMMDENhcmxvcyBBbHZlcz
EnMCUGCSqG
SIb3DQEJARYYCgQOMTg0MEBhbnVub3MudW1pbmhvLnB0MIIIBjANBgk
qhkiG9w0B
AQEFAA0CAQ8AMIIBCGKAQEAnH11lrRc/m0M1Wwz5tzTqfIqYp/Dc9MD
hh0/N9uI
8PKrw1afNZBN6jC YadgHMkony0dir/04pfK6EJ2DDQ2mZnah809TTOIS
c+8f1YqY
wehh24B5FLpN2xazX0gKZYHdRB6lnC3BWGSk24W0nmi5BAkuhq22qPc
UbK+fnudr
beEfwUadGahb0SwhB7pTLZ5z1kWdXP+ImPIsMhaszkhTKz+zg7Ui9wM
SUMdvMwU0
H4HfEIQRkR/rK05Fh0iViRQayh8KvftK2gzjkVoPCOF0tQZqlQZtqmD
jXNmN9ffM
gyQ0XtwxrK4f85fdsKzd1257d0Aw2QgWZYwVw4FHEtAF7QIDAQABMA0
GCSqGSIb3
DQEBCwUAA4IBAQAUAHbHhZhcSi8fZrJ9sA1jsVPfEdkZhuV69JR0TIM
2gj/zAPhg
aQtsnPSAabb6/0uzMv6tEJQDaAYXa7HLIA9PpbIqaKqLNs40VSHe0iV
CEX7T0uRP
7yqm9yLEADRLyg1KCszTTByCj64y0alninMY3jNlSpx9RITsHlqknkv
zUqKQ+A5
4Z55N5oZzLMoclr79iMR0R8d06Cq8sXEXkCsxw6Jb5AyCziab7s1+a/
26m0sk7Cj
Pug69ZSxfalB1Lb+Qigi0e0geM49gbjE8i3cQE0XTZBHQrpWZTNGHYPC
gf0zueC
y5xvBG6YjIKMxKixTWvrFoJvCB973DkQizSg
-----END CERTIFICATE-----
```

Figura 13. Verificação do ficheiro com o certificado auto assinado



## Alínea 17

No quesito do desenvolvimento da PKI decidimos utilizar a implementação sugerida no enunciado, deste modo fomos capazes (todos os elementos) de submeter o pedido de certificado, onde recebemos o nosso certificado assinado e ainda descarregamos o certificado publico da CA de modo a verificarmos os certificados assinados pela CA e por último a opção de revogar certificados (usado na última alínea).

## Alínea 18

Obtendo o ficheiro PKCS#12 e verificação do estado do ficheiro com certificado assinado e a chave privada.

[illegible]

Figura 14. Verificação do ficheiro – Carlos Alves

[illegible]

Figura 15. Verificação do ficheiro – Bruno Rodrigues

```

openssl pkcs12 -info -in priv-pkcs12.p12
Enter Import Password:
MAC: sha1, Iteration 2048
MAC length: 20, salt length: 8
PKCS7 Encrypted data: pbewithSHA1and96bitRC2-CBC, iteration 2048
Certificate bag
Bag Attributes
    friendlyName: Paulo
    localKeyId: 21 EE 45 90 D1 E0 E0 11 0B FF 63 9F 95 43 25 81 9D A7 1A
subject=C = qw, ST = qw, L = qw, O = qw, OU = qw, CN = qw, emailAddress = qw

issuer=C = PT, ST = Braga, O = Henrique Santos CA, OU = HS CA, CN = Henrique Santos CA, emailAddress = hsantos@dsi.uminho.pt

-----BEGIN CERTIFICATE-----
MIIEMDCCAXigAwIBAgIJAMKkiylEue45MA0GCSqGSI3DQEBwUAMIGNMqcWcyD
VQQGEzQVDEODMawGAUECAwQFnJhZ2ExeGxzAGBNBAOMEkhIbnJpcXVIIFNhbncvYD
cCgBDQTEODMawGAUECWwFSFMgQ0EXgzAZGNVBAOMEkhIbnJpcXVIIFNhbncvYD
QTEKMICGCSqGSI3DQEJARyVaHnbnRvc0Bkc2kudUtpbmhvLnNbMB4XDTE5MTEx
NDAlMTEXNTODtIMTExMZA1MTEXNTowYTELMKA6A1UEBHMCcxCAAJBGNVBAGM
ANP3MQscWcyDVQQAjxZELMKA6A1UECGwcCxCAAJBGNVBASMANP3MQscWcyD
VQQAjxZdERMA6CSqGSI3DQEJARyCcxcwgEIMA0GCSqGSI3DQEBQUAAQ1B
DhwaggeKAOIABaQcdIfLxnbm+1qb5TV3kyMb+PKabZufK74rSe65DQMhEKbVzae
+JebvgvhdiDVCjdayLnqNZxpZFBB3o5u+y47YLULsKa91658d7XFqzJD0af0f
0gcCR9+r3Z3TrqYPqbe0lvff7nP7PfFuU3yx2RElJct+sB5/82zxpkvt7+Fee
+ATZ/cuhv3vbW45Xu+aqS1MD7Zaa8mban0ns719rg0gKHip6EEYioUb/q4QuX8
ITPLPA1fSD6QAISMYIurVzu2ZEpfvkrZu/kva9ryJIMEC48dfTXnaHu8E4JFO
PPFEIN15wTmc8I4f3QuZoXSxKhFBnJahdzagHBAAgJgb0ugbowPwyIKuYBBIQH
AQEENZXmC6cc6GAQUBZABHInodHrwidlvb6gf1c2VjaW90LRzaSS1bulua68u
CqQBzhMZHTAJBgNVHRMEAJAAMCWCSCMGSAAG+E1BDQQfPh1PCgvUU1NHIEDlbavY
YXR1CBSDZXJ0ZWZpY2F0ZAdBgNVHQ4EFQgUBYxyQocXcoycvm85VcllALBRduOw
HwDYVR0JBgBuFoAU21lr/P3twtfAh/ItiADsRonrowwDQYJKoZIhvcNAQELBQAD
ggEBAEilr+iR7vNXaiC6ajhxILtJRgl1iid0OfHfp4J40DlnawdoXoxkuBVYCnV
a0F3gwuE+mqsYR4Pz683W1XYRUDb6y1fhmuGP3HNWSHEQka8bhJ07twHbdOL9IN
fBSZseuEPFTHz/JJVbvTF+q6RWyf/ddyq9u1okxmTgyrfmZS25MHAFPDmhndsr/p
dtb4wlHwh10JxwCLTR5kl1nnbehuxlzzeCGK5c5SySceuat9rm1gp2VikBLTA34Y
Y/+LVgdLKQLXL1J3r85HZaeYd5b8qHarMLB0hx+QLPBHF1CYkxlyx/zrye/2rje2J
1QHhsKcc/xvih60Jjh3r1Skgnmc=
-----END CERTIFICATE-----
```

```
PKCS7 Data
Shrouded Keybag: pbewithSHA1And3-KeyTripleDES-CBC, Iteration 2048
Bag Attributes
    friendlyName: Paulo
    localKeyId: 21 EE 45 90 D1 E0 E0 11 0B FF 63 9F 95 43 23 75 81 9D A7 1A
Key Attributes: (No Attributes)
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----BEGIN ENCRYPTED PRIVATE KEY-----
MIIFHDBOBgkqhkiG9w0BBQwQTApBgkqhkiG9w0BBQwwHAQIbDbMQYNF5CR4Cagga
MIIFFCCqGES1b3DQ1JBQwFAYIKoZIhvcNAwECLT81OC29kHAB1Eyc561oSkuHsM
ybdN3NY50hfDVTHnetuMd8z139dpEtZCBb71PP0TImoi3Dnb4QWPO/PDXUHWLISx
6x21cpme5EjQ0oJv1C3UoVa2Y1Cub1SwDcrb6L1p6x850MmYau2xVKRYX9UntTqS
b6Ye00v1DqHXCPNQLOQRud3p0fpbbYL1fGETkouZlpzJkeALa37LyR4yz4os81E
ayJDRn7E1FzLTl7G5tAg5TP3R+a9njn0mJzs6Q8/KFipnQ1s3V36CmGr4YxvW
Vhp3tnwadUkcTDQVZLi6bk6608+rTeuWJX4ic/DWxH2vbgAEqP11mftKJzoVlCS
gFSFmV9ce2Qlr63Wt2Uelr82DgurLz131UQCvyFcSap39/4aTx20eKLVj0FGDP8
LKnw5Jve+ahwLq5B1TFTFYph2NmxOUUrFj+MkwLn1XEMc35mBk1f2rKR1A/7w1uW
3yh2p4jhF5MqsdBynq41EbkaXb+YE10x8FQqVFMh/SJ+fFgnoY9mKK012FM/pn1
FF6mqg2vgQWwqn4s4bYL2xc1H3dMNDkg1DK7kys6hr6p6NyKpyYM6rBBj82TnkKE
2rpxwcvq1J3dedDvc+u00Fxn9s3v17PDN86UtoCaBeKJbKy14sJe6WkR0wpdLM3D
u3/5LR4mQwue7p12341m68aqZPoiedCts5bv6c6fsTp/1+Lg1JtDe638QZuygJFR
p06a1HC4WqrLz1245EBY8rTjfkLSCQ1Tjnen1gc6Nh5Es2V21fb1tUn6p9sqt1y
25TKXvpm8AefzZu41rljwBAWz3WdqvZ5p6zW7sVqPULy2/+88m19RyWfRGmURCMj
qALHBA2GyrJ0sJ/s+m918il806fWu6z33BF6FM8y0fL2MYamfvYe1r9JYeedWBT
31AWJ8ks1S8e+sHsz5Uj3Kp6AJ/1U0U3ZKEjP5Xeo0wtrH1FuntRn1iK1BH80
gvvz1e7Uht0ixuJrJpF4hN1TD/NJJKwmqQZFMHRapf1ru18JnoAH5/aXvTM
3/fuCiCYMLsRj6a1vcgDzW7FX4aSRaV/5odyx9+cQ+r7nWdQ/kY2QZp1b359kBU
ZBpxQD/rJgXNEEQ7st+d412B7MHZqwmPYuX9X0EVU1KrBkCw0iQJADJT2MkdKdAt
iF76fu4o/mKaym8A1b6a+uHu+bFV08ZNpBsJp3PTTUeEz2u0Zd2e4XqfpmH7
D14SEYRLlga62xk21x5MwduTY5KA/KV2xQ25P52qzvdSx7Hjr2aijrUTSM+1Dh1
VCCVsu1621un9a0ZahHbc6b6kDMWqgFbyJZn4f516ktY010bkys16axXUSP504sn
y/Pxxdam9QrPy5bDZpCegMSY1Q5JWbQaObT+JqYtQz13R5f8gURCR86SfG/5bEA
ueK1WkA5FuW2P5bEAnPD59R8o1M31jxtZLu1NjK1iRSR8UuLXf5a6L6f3xv9CTs
Yq5hCwgK2B13a1PwbnJeP/Jv52kVdf9nPPH/vM0srow/6amqinLvEuyH1EXusmU
WpkYAgfoHo7Sa9a64hfXrQhsQdm65f393/5ad6YHBIku+qH7XOUVZNg31BVxxkd
deghyzbordJJ61J6X1PX1Q==
-----END ENCRYPTED PRIVATE KEY-----
```

Figura 16. Verificação do ficheiro – Paulo Bento

Em relação a diferenças entre este resultado e o obtido no passo 4, é a encriptação da chave privada, a inserção de elementos criptográficos como MAC, número de iterações, e ainda *salt* para promover a segurança do ficheiro.



## Enviar e receber mensagens seguras

Instalação dos certificados por elemento de grupo:

Carlos Alves

*Tools -> Account Settings -> Security -> Manage Certificates*

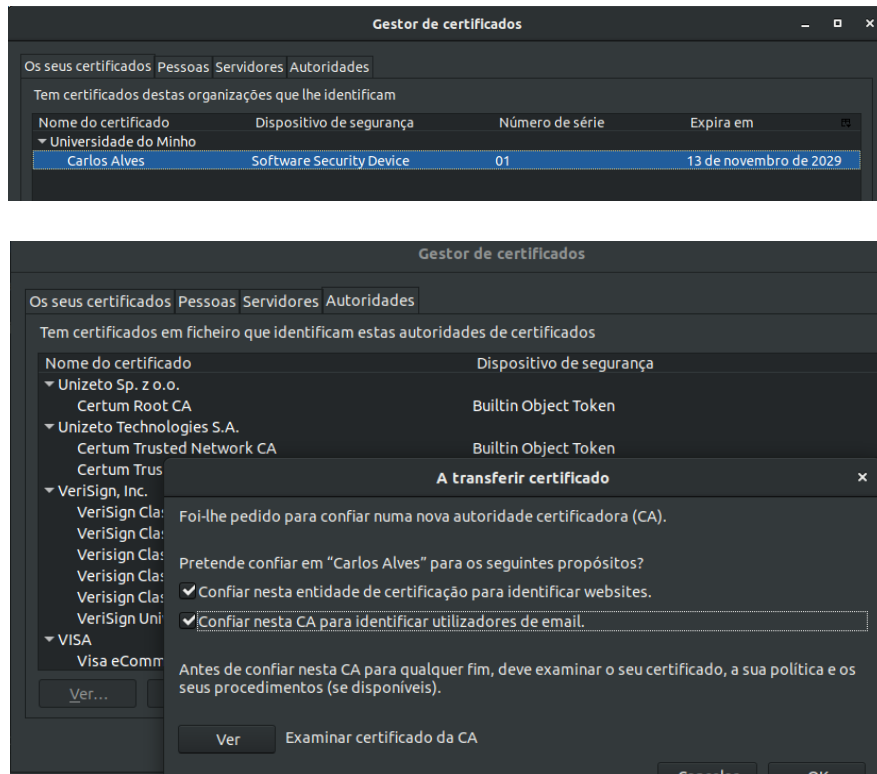


Figura 17. Importação do certificado X.509 através do ThunderBird – Enigmail.

*Enigmail -> Key Management*

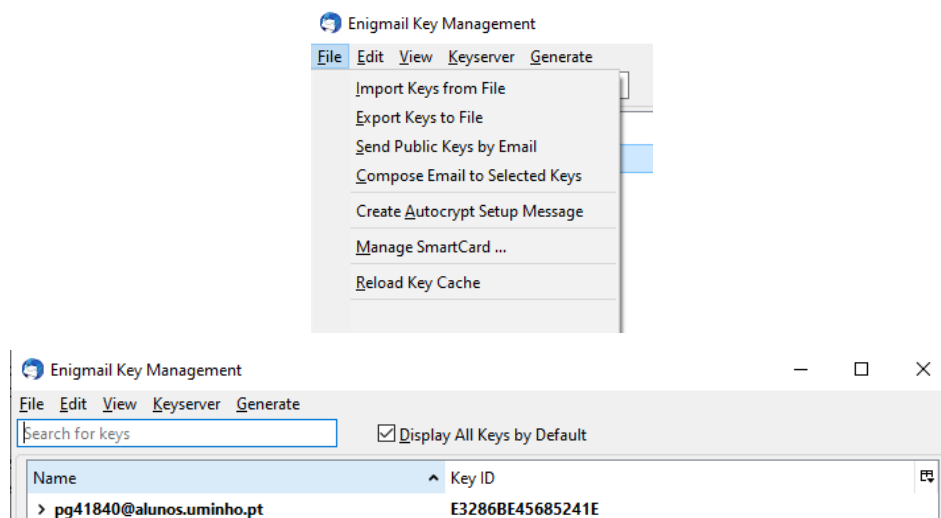


Figura 18. Importação do certificado PGP.

Bruno Rodrigues

*Tools -> Account Settings -> Security -> Manage Certificates*

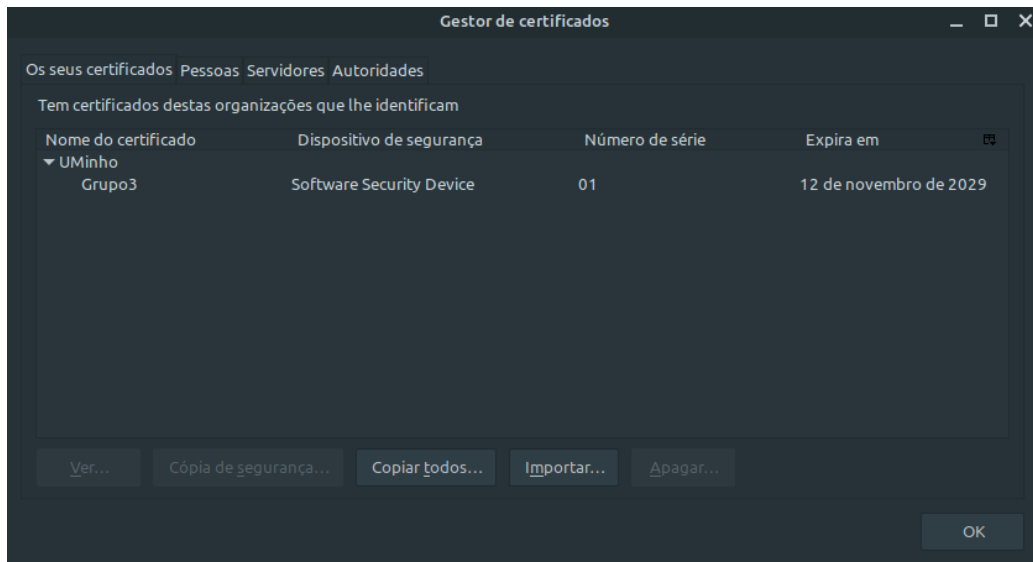


Figura 19. Importação do certificado X.509

*Enigmail -> Key Management*

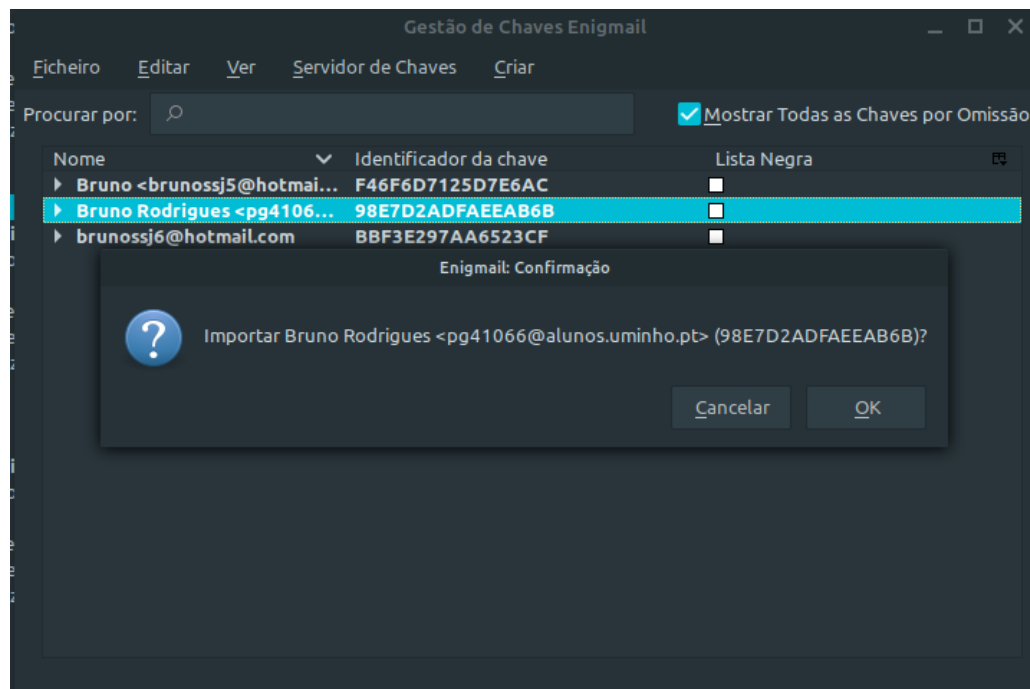


Figura 18. Importação do certificado PGP

Paulo Bento

*Tools -> Account Settings -> Security -> Manage Certificates*

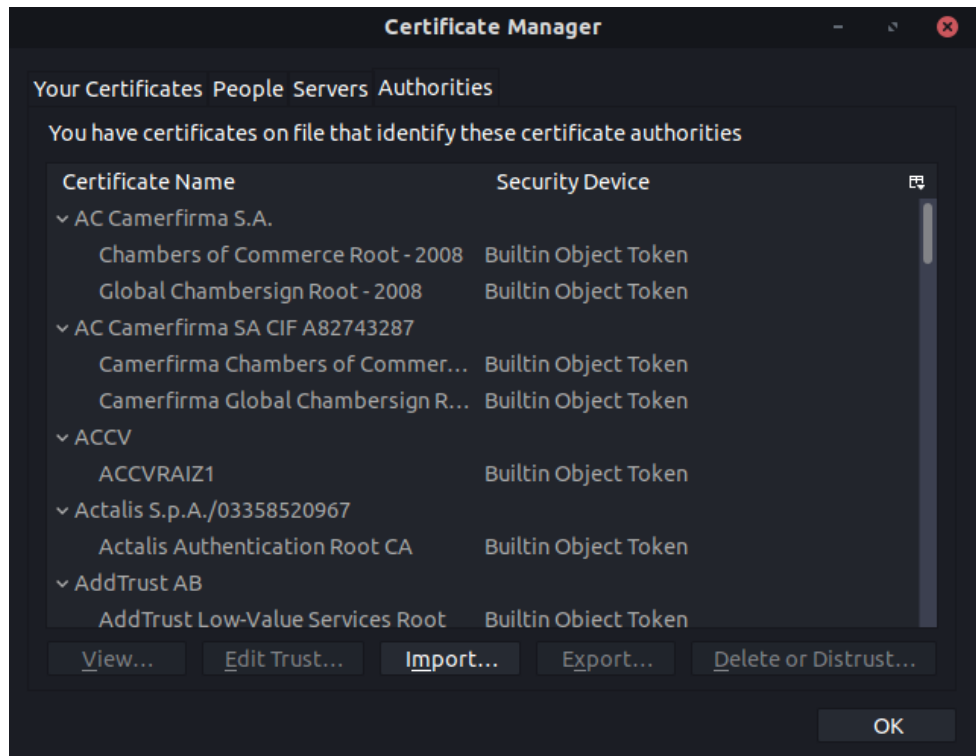


Figura 19. Importação do certificado X.509

*Enigmail -> Key Management*

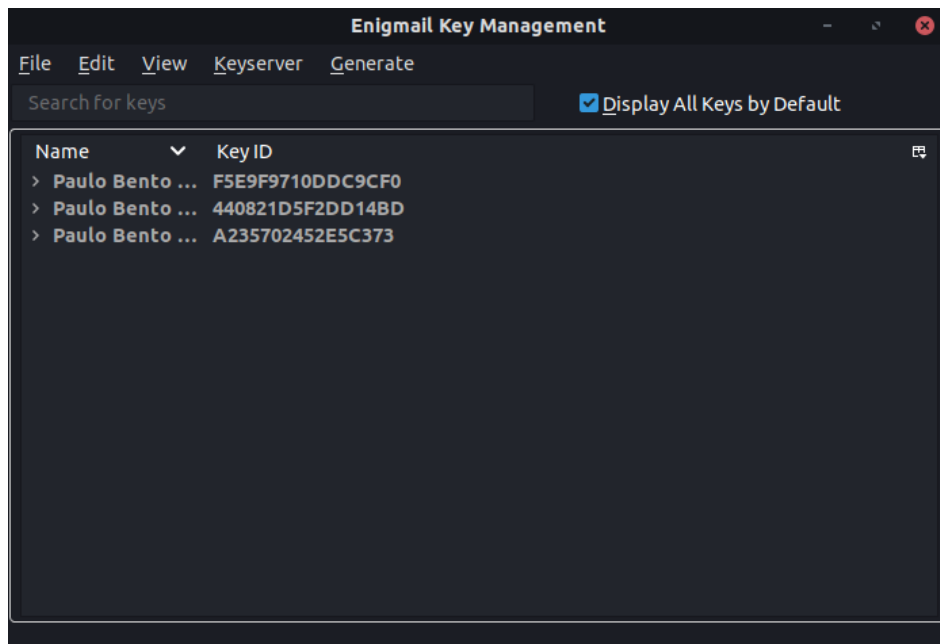


Figura 20. Importação do certificado PGP

Alínea 2  
Carlos Alves

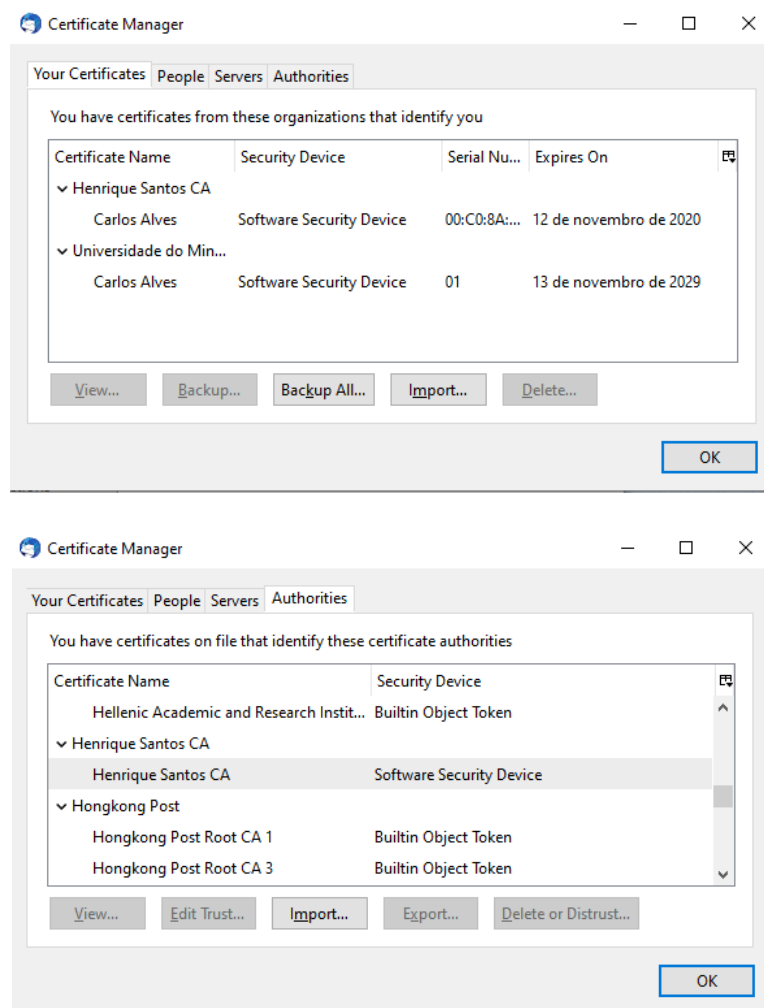


Figura 21. Gestor de certificados (Meus certificados e Autoridades)

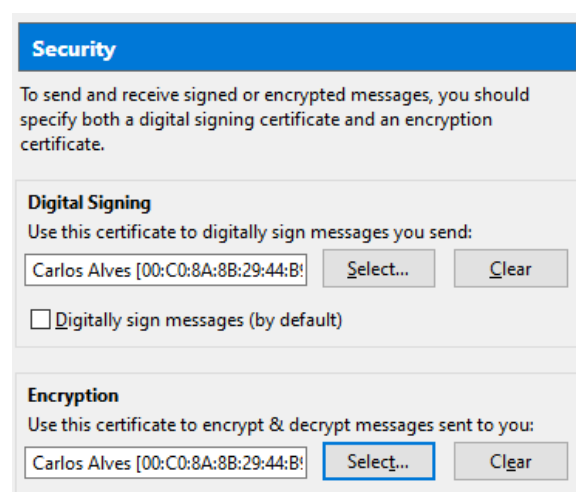


Figura 22. Escolher certificado

Bruno Rodrigues

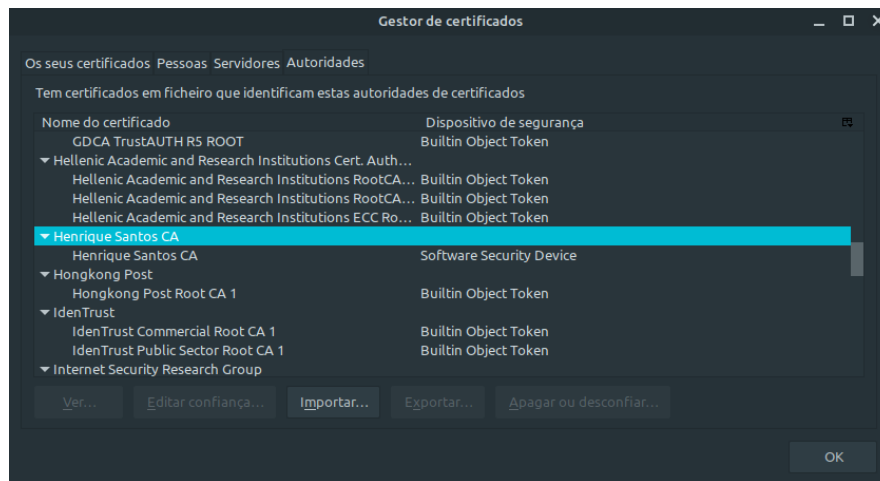
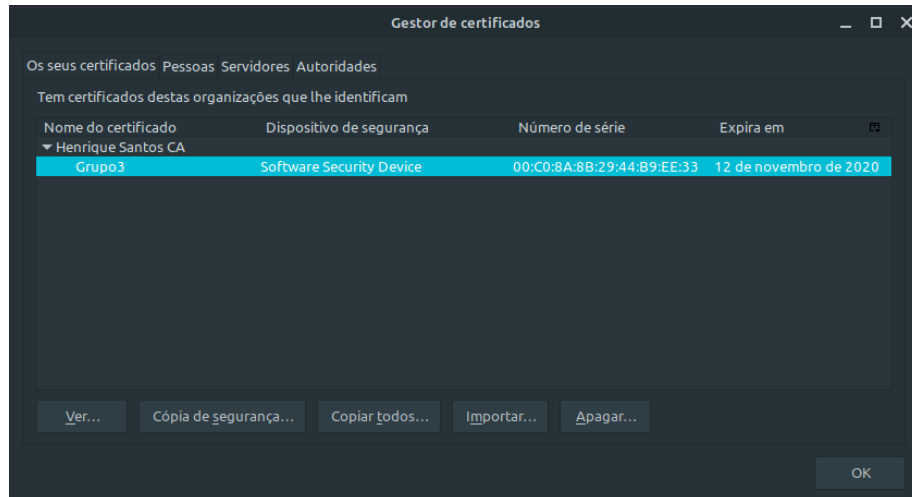


Figura 23. Gestor de certificados (Meus certificados e Autoridades)

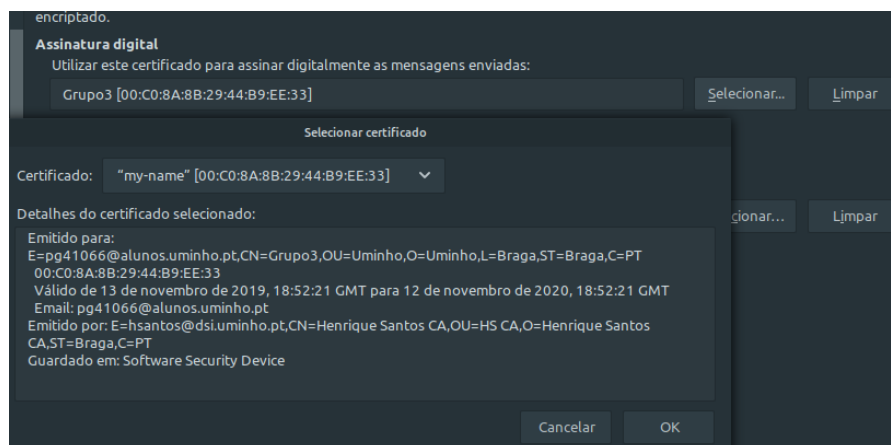
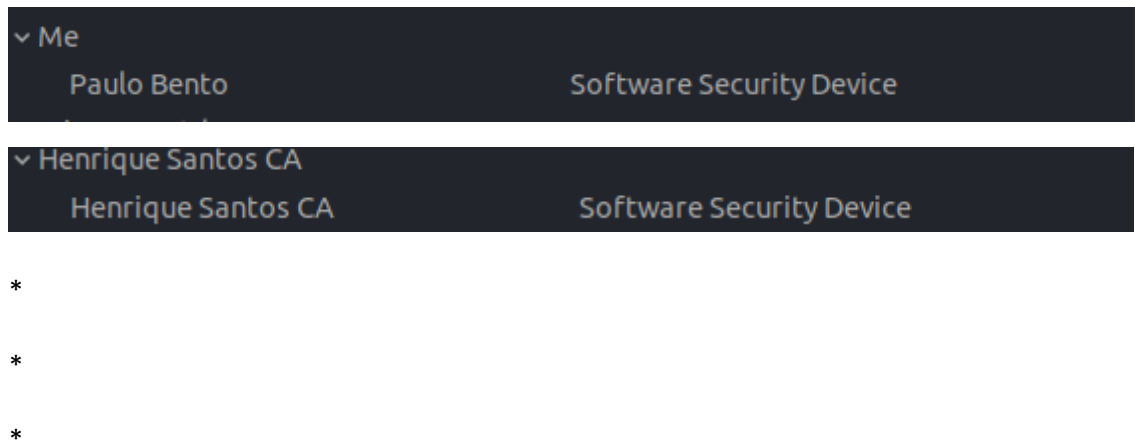


Figura 24. Escolher certificado

Paulo Bento



### Alínea 3

Envio de mensagens entre os elementos do grupo. Nesta alínea cada um dos elementos enviou um email para outro elemento, onde o email se encontra encriptado e assinado.



Figura 27. Encriptar e assinar a mensagem

### Mensagem enviada de Carlos para Bruno

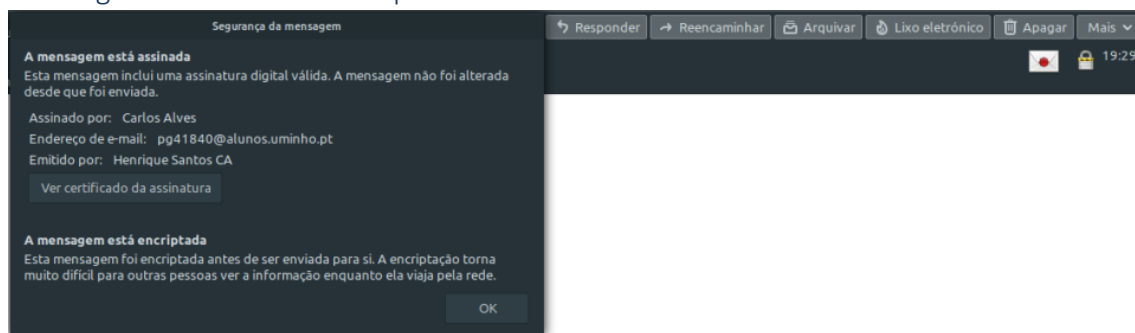


Figura 28. Verificação da mensagem enviada por Carlos a Bruno (assinada e encriptada)

## Mensagem enviada de Bruno para Carlos

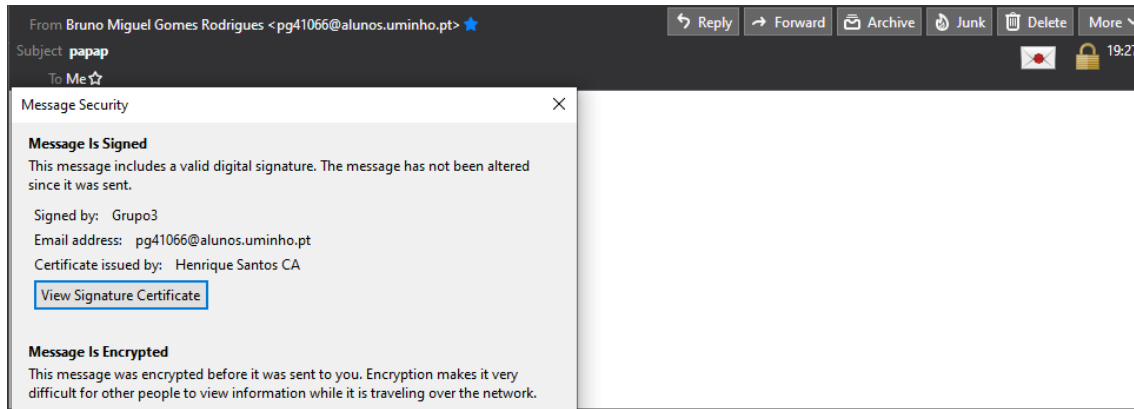


Figura 29. Verificação da mensagem enviada por Bruno a Carlos (assinada e encriptada)

## Mensagem enviada de Paulo para Bruno

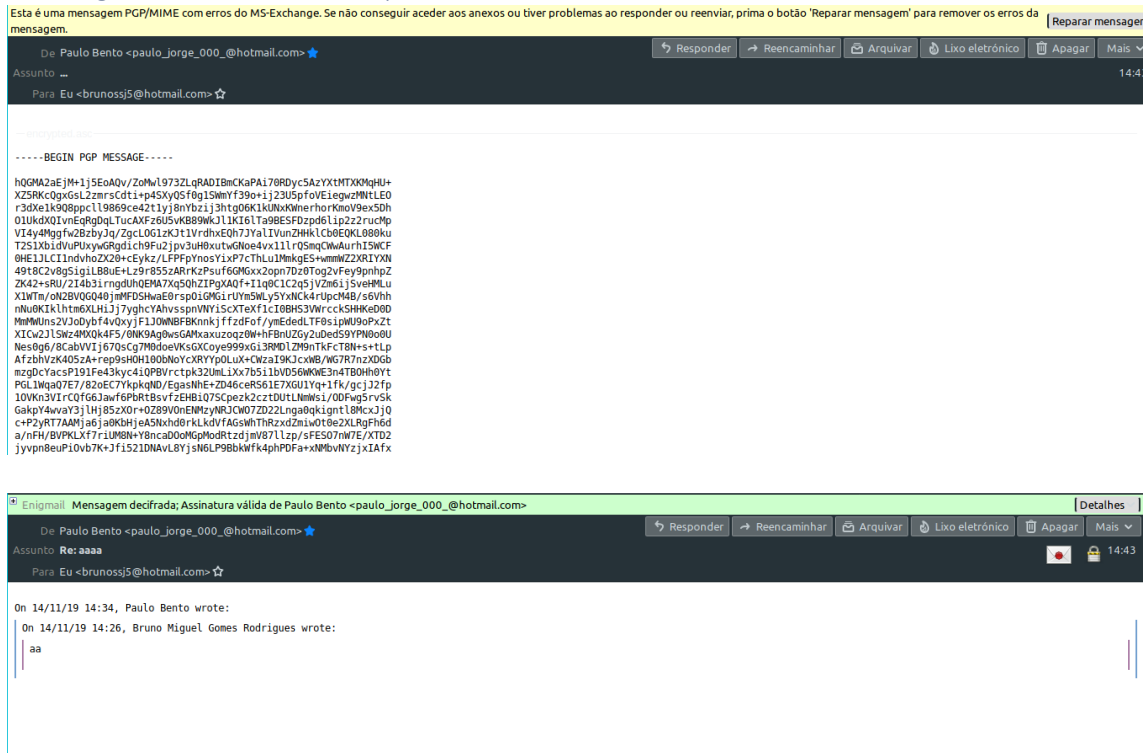


Figura 30. Verificação da mensagem enviada por Paulo a Bruno (assinada e encriptada)

## Alínea 4 – Revogação de certificados

Poderá usar este certificado para tornar segura a comunicação com os seguintes endereços de e-mail:

E-mail	Nome	Nível de Confiança
pg41840@alunos.uminho.pt		✓ total

Adicionar um endereço de e-mail   Mudar a Frase-Senha   Gerar um certificado de revogação

Foi criado o certificado de revogação - ... ? X

**i** O certificado foi criado com sucesso.

**Note:**  
Para evitar uma importação sem querer da revogação é necessário que edite manualmente o certificado antes de o poder importar.

OK

Figura 31. Criação do certificado de revogação

```
bruno@bruno-Aspire-E5-575G:~$ gpg --output revocation_certificate.asc --gen-revoke FAEEAB6B
gpg: enabled debug flags: memstat

sec rsa2048/98E7D2ADFAEEAB6B 2019-11-06 Bruno Rodrigues <pg41066@alunos.uminho.pt>

Gerar um certificado de revogação para esta chave? (s/N) s
Por favor, selecione o motivo da revogação:
 0 = Nenhum motivo especificado
 1 = A chave foi comprometida
 2 = A chave foi substituída
 3 = A chave já não é utilizada
 Q = Cancel
(Provavelmente você quer seleccionar 1 aqui)
Decisão? 0
Entre com uma descrição opcional; e finalize-a com uma linha em branco:
>
Razão para a revogação: Nenhum motivo especificado
(Nenhuma descrição indicada)
É esta aprovação? (y/N) y
Saída com armadura ASCII forçada.
Certificado da revogação criado.

Mova-o por favor para um meio que você possa escondê-lo afastado; se Mallory começar
o acesso a este certificado pode usá-lo para fazer sua chave usável.
É interessante imprimir este certificado e armazená-lo afastado, apenas no caso
de seus meios se tornarem ilegíveis. Mas tenha cuidado: O sistema de
cópia de sua máquina pode armazenar os dados e fazê-los disponíveis a outros!
gpg: keydb: handles=2 locks=0 parse=2 get=2
gpg:      build=0 update=0 insert=0 delete=0
gpg:      reset=0 found=2 not=1 cache=0 not=0
gpg: kid not found cache: count=0 peak=0 flushes=0
gpg: sig cache: total=2 cached=0 good=0 bad=0
gpg: random usage: poolsize=600 mixed=0 polls=0/0 added=0/0
gpg:      outmix=0 getlvl1=0/0 getlvl2=0/0
gpg: rndjent stat: collector=0x0000000000000000 calls=0 bytes=0
gpg: secmem usage: 0/65536 bytes in 0 blocks
```



De seguida foi feito o *refresh* aos certificados de modo a atualizar todos os certificados existentes.

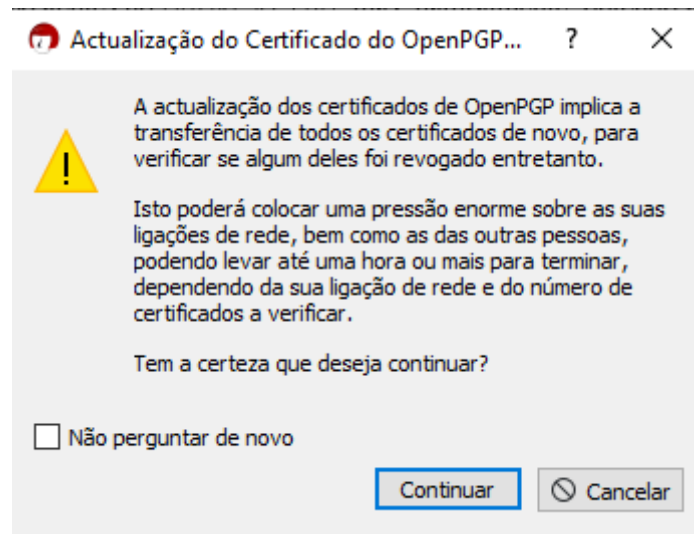


Figura 32. Atualização dos certificados PGP

```
Using configuration from /usr/lib/ssl/openssl.cnf
Revoking Certificate C08A8B2944B9EE33.
Data Base Updated
```

Figura 33. Revogação do certificado X509 utilizando a ferramenta fornecida no enunciado.

No caso da revogação do certificado PGP observamos que após a revogação, não nos foi permitido enviar emails. No caso da revogação do certificado X509 não verificamos quais quer alterações, visto que ainda conseguíamos enviar emails, o que supostamente não deveria ser possível.

## Proteger documentos locais

Seguindo o enunciado escolhemos um documento que desejamos encriptar, configuramos conforme é possível observar na imagem (qual assinatura e para quem é que iríamos encriptar o ficheiro), por fim temos o ficheiro encriptado. Tivemos a possibilidade de usar as opções do *GpgEx*. As imagens que se seguem correspondem a todos estes processos.

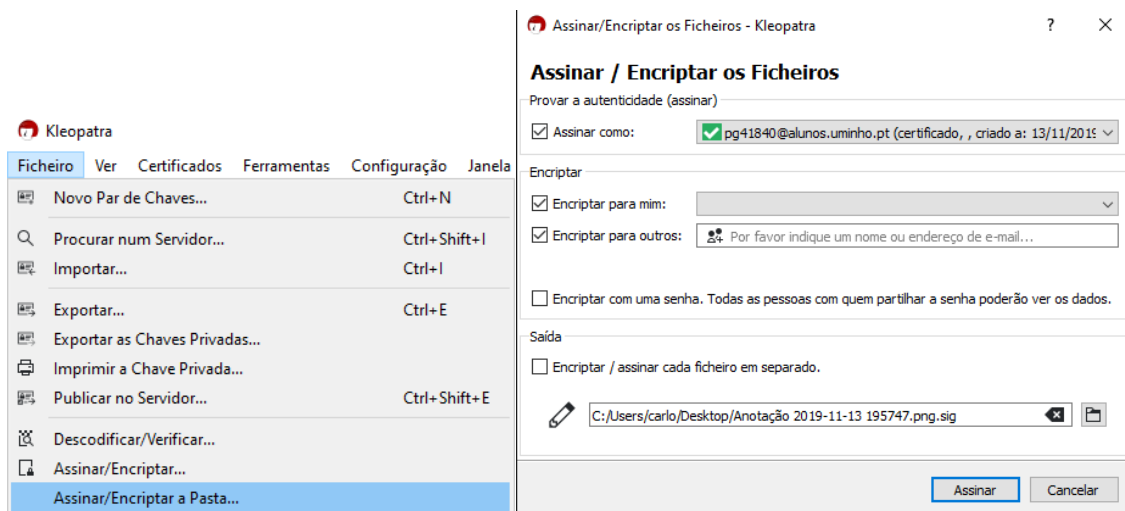


Figura 34. Assinar/encriptar ficheiros usando o Kleopatra

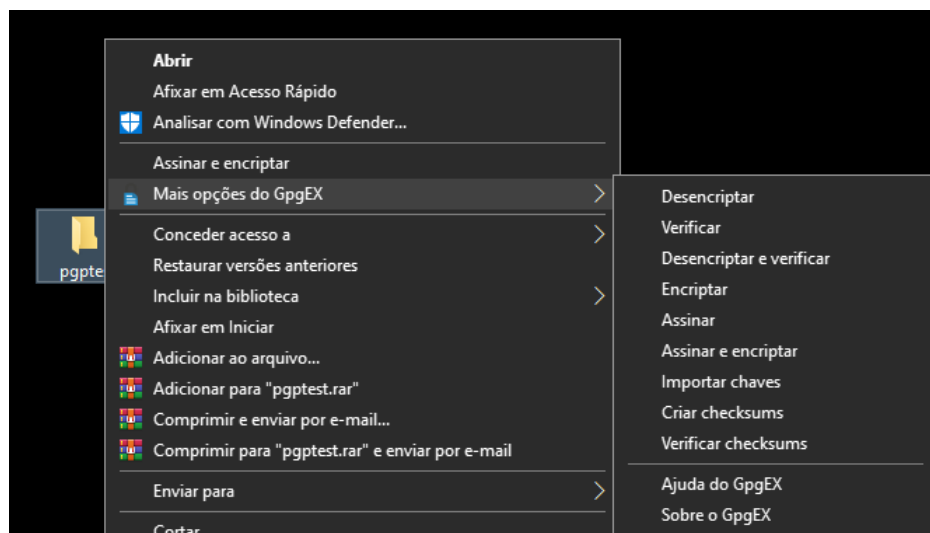


Figura 35. Usando as opções do GpgEx

## Conclusão

Neste trabalho abordamos diferentes mecanismos de encriptação com uso de chaves simétricas e chaves publicas, com ênfase na troca segura de emails.

Foram utilizados dois métodos que possibilitam e permitem manter a integridade e a confidencialidade dos emails trocados, a utilização do PGP e de certificados x509, sendo que foram criadas chaves com recurso ao programa *Kleopatra* e a criação dos certificados com recurso ao *OpenSSL*.

Era como objetivo neste trabalho descrever como estes conceitos de chave publica são implementados, compreender como estas são geridas como também conhecer e saber utilizar as ferramentas que existem e que permitem realizar a gestão das mesmas.

Acreditamos que todos os objetivos pedidos foram cumpridos. Todos os elementos do grupo criaram as suas próprias chaves, como também os seus próprios certificados. Cada um dos elementos procedeu também ao envio de emails encriptados e assinados, utilizando o Mozilla Thunderbird e a ferramenta *Enigmail*, a todos os outros elementos. Não podemos agora deixar de mencionar que um dos passos pedidos, mas que seria opcional, a criação de uma **Pki** simples, não foi cumprido por nenhum dos elementos do grupo, sendo que todos utilizaram aquela disponibilizada pelo professor. Uma das razões para tal foi que um dos elementos do grupo encontrou problemas técnicos durante a realização do trabalho, que atrasou o seu desenvolvimento, e como tal os elementos decidiram utilizar a **Pki** existente.

Não obstante, acreditamos que a realização deste trabalho foi importante para o aprofundamento e o entendimento no uso e na implementação de técnicas criptográficas no envio de emails, um dos pontos lecionados durante as aulas teóricas.

## Referências

Alfred J.Menezes, P. C. (1996). *Handbook of Applied Cryptography*. CRC Press.