Universidade do Minho

Escola de Engenharia

Mestrado Integrado em Engenharia de Telecomunicações e Informática

Segurança em Redes de Computadores

Trabalho Prático Nº 2
Cifras, Assinaturas, Certificados e ADSS

Elementos do grupo:

Hélder Duarte A75121

Hugo Pereira A48319

Manuel Coutinho A76569

19 de Março de 2018

Índice

Parte 1 – Gestão de chaves 4

1- Importação do certificado de grupo. 4

2- Instalação do openSSL 5

3- Gerar o par de chaves para cada elemento 5

4- Gerar um ficheiro com um pedido de certificado 9

5- Gerar um certificado auto assinado (X509) 15

6- Criação da Autoridade de Certificação 16

7- Configuração da CA 16

8- Detalhes do certificado 17

9- Configuração da CA 18

10- Assinar os pedidos de certificados individuais 19

11- Verificação dos certificados individuais 21

12- Gerar o ficheiro PKCS#12 25

13- Instalação de todos os certificados no Sistema Operativo 26

13.1- Windows 26

Parte 2 - Enviar e receber mensagens seguras 28

1- Inserir o certificado P12 no *Outlook* 28

2- Importação dos certificados pessoais para o Outlook 2016 29

3- Troca de emails encriptados e assinados 30

3.1- Entre elementos do mesmo grupo 30

3.2- Entre os nossos elementos e os elementos do grupo 3. 31

4- Revogação de um certificado. 32

5- Resposta à pergunta sobre outras possibilidades sobre a criação de relações de confiança entre diversas CAs. 34

6- Conclusão 35

Índice de figuras

Figura 1 - Importação do certificado de grupo. 4

Figura 2 - Instalação do certificado de grupo 4

Figura 3 – Criação do novo par de chaves. 16

Figura 4 – Criação do certificado do Grupo2. 16

Figura 5 - Detalhes do certificado. 17

Figura 6 - Configuração da CA. 18

Figura 7 - Assinatura do certificado do Hélder. 19

Figura 8 - Assinatura do certificado do Hugo. 19

Figura 9 - Assinatura do certificado do Manuel. 20

Figura 10 - Assinatura do certificado do usertest. 20

Figura 11 - Vista geral dos certificados individuais. 21

Figura 12 - Comandos para criar ficheiro PKCS#12. 25

Figura 13 - Gestor de certificados do Windows. 26

Figura 14 - Pedido de password para importar o certificado. 27

Figura 15 - Importação da chave privada (p12). 28

Figura 16 - Importar certificado pessoal do contato. 29

Figura 17 - Pedido da password para aceder à chave privada para assinar um e-mail. 29

Figura 18 - Email enviado encriptado e assinado por um elemento do grupo. 30

Figura 19 – Email recebido desencriptado e digitalmente assinado por um elemento do grupo. 30

Figura 20 – Visualização do certificado e respetiva assinatura digital. 30

Figura 21 - Email enviado do nosso grupo para um elemento do grupo 3. 31

Figura 22 - Email do grupo 2, recebido pelo grupo 3. 31

Figura 23-Revogação de um certificado. 32

Figura 24 - Certificados após revogação. 32

Figura 26 - Importação da nossa CRL para o nosso computador. 33

Figura 27 - CRLs. 33

Figura 28 - Incapacidade para encriptar mensagem devido à falta de certificado. 33

Parte 1 – Gestão de chaves

1- Importação do certificado de grupo.

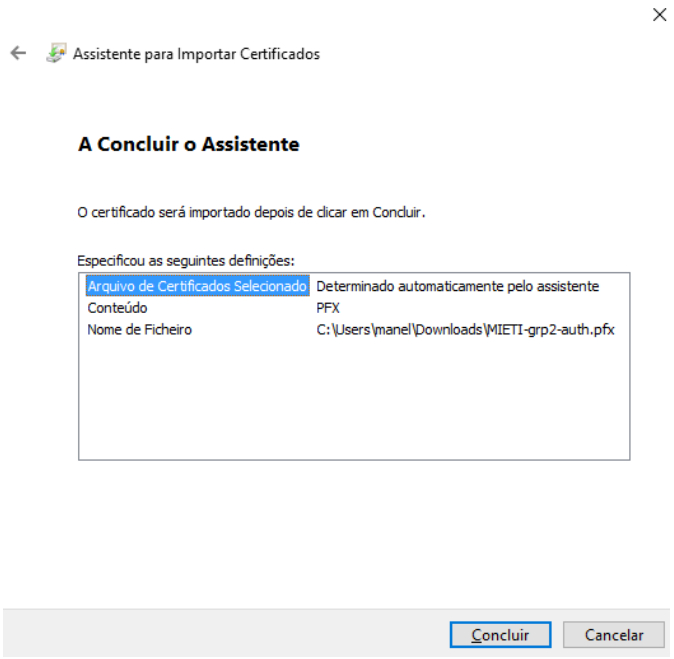


Figura 1 - Importação do certificado de grupo.

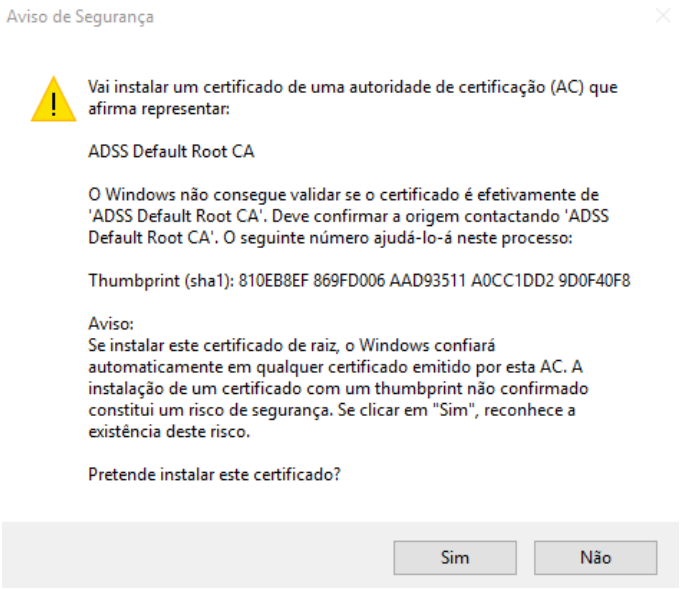


Figura 2 - Instalação do certificado de grupo

2- Instalação do openSSL

Foi utilizado o openSSL pré-instalado no sistema operativo Linux

3- Gerar o par de chaves para cada elemento

Após reunião de dúvidas com o professor ficou acordado a criação de um 4º utilizador para o grupo, na tentativa de corrigir uns supostos erros no ADSS. Erros esses que mais tarde se verificaram que apenas se evidenciavam no servidor de ADSS.

Objetivo: gerar o par de chaves RSA

Comando: openssl genrsa -out privkey.pem 2048

Objetivo: verificar o par de chaves

Comando: openssl rsa -in privkey.pem -check

- Resultado do Hélder:

RSA key ok

-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAmnj18FUdJ3BClR08HiiXumrIKicd/sCd+tGJOlN7mphEd0wy
mXvC5eR32BSPBjxVyXsrjv0hQ3eOSW8kDcqiuzcxZYUm61T9fczAPvw7YV+sQzm
34iquiR3FGAwx1Om560Gv9sUaCSwP1Xv/Hw25xXRVlW8o+GR3yo8hFrTVv9AktZ
BN3ZgT3d4dQfPZaJaDEpBwxLmm3UTrMT8Rt1UB4EljonOLpeshAxW+/KQwuzyV
GqUmSMpAbcknfzVYrJQ040xX0w/plQT9zFEbZvTE3sbUdXXhGHCr93xgEhyFlPtP
WDGZ6/OXskhvZ+MPJMgS1QTJiVJZuq4O2sNkF+50DQIDAQABAoIBAQCU6Yrd
do+2V0g4i4hK4oLyWMJBsJf/4BvrkVei/JupeqR2BOS6hU5rZIYLrjX6outoYe6p12fbr
ENkk1nEWdXqeNiLr4LHVpVQUrP5hBqSUjK0U83qn47F7Ab2mbroL7DlE9vYHkZt
FSbmfLSCcS7nJLDkb9alLeU1Ril1xDpSv4s8Kcrwy7EkM4lssy5WIhTRCIiLWr/+Y1e
s903fwWDuJQUZ7P++53SfAbkAB5B47q0mO6F0zXLWtCsT7mZH6MrUY9LcoGD4
wWx7iR7n2DIFaGCoCYjO/1DurCi9a5Hoap5zFLIkXeNKbIMzZ4mxCBVQIm8W42n
Sb5N+wSjeJ+OZAoGBAMvv6x2dXPKGXuknH7vzeYniN3KbhsH+qaIALagkHpum/e
EZVLflT6vcDpg9F2BkEG/NTXFv6bcS1elbAHJpCgo6HkwwrsxqkbbzjxGYoeGGwxp
etLnHvr4v0aiGpssbTPw6hVJVYaTOWOM7cwowMuf4m+jOceLNwWA6kvIufGejAo
GBAMHoVa7ThStgBQcgS9+BJ3be4T+gTrOoLJNiImEDSXUUnbZ0ZdpK8n9YdA/p
dDlX2Tlv5TBX9jNBwB9/3bDGjdvu1wbb8h0nMu7yJlEFUEuYrOppcJI684YKIdVN/0
o3sgIufg6ctGzKcOokC/6I30cksvwZqQFiaXPzaE7XFjCPAoGBAKjDwFPfl71ziTN0lw
RYtilutOf44InFjudrMl1ElrfEd7BB4CPWdhoIn2NImwG/jQKYaRAIxuYjhjX4guQrHI
3eDpiKaPzs6+z0nV64aq5RcT9vRCvBqo2E0QGffIPz8b+BRjceRRG3WUOiPM8fl+D
zkUIVJZXFI9PYZSZZZcX1AoGAcfra2sAU6FExw2WVk9R8WSBb8SWO/YXeZefq
Y3ImLL8okYZMFIu3jWl2F6BXpBliY6PFaaxa2PhOMXXc3ztnSZ9UIAELiV1wUAp
gwYFJGJavFb9S33HtkZ3FE3gclwi0BxpDGN2+JLC+vLLhpgXYkR4eY5fFwz2Q1Qq
ABs/hiDsCgYA7oPnmpgmMlj8t81O/MxDqMIgP5SpAqlqTIAG+X2njlachnksKqCjW
2ihSh/Vt1UF/uaqjyZNw4vw43EY9a1z0zOqTISsLzDTHqVN9Zb+WngLFHvs58XXb
sY7rOd2KSmyqvsVWtatTQroCMZ78wQh85quimdlod32FgqB84Fo+8g==
-----END RSA PRIVATE KEY-----

- Resultado do Hugo:

RSA key ok

-----BEGIN RSA PRIVATE KEY-----
MIIEpgIBAAKCAQEA4lNhFXaq7CZZqa+d79jC2UHXhDrTQT3oxYBaJSW7CzzNc
CzPQSEpAZJxyCwPRXoacmGcKKalJ90tC7KSK+Dz3A17jFFnVjxZStqfSuulpmgRC
k291yVfh0gPxqFFlRAuO+vlma+R7CHjG5fZmFi17zNLf/aintWccRpMn6BpYtlZIPze
BhPinKyJDkTnX9S8Iq/ZTzn4385NXjQWztqsBkRnFb0q2uuNQqUhZ8prY5oykDtBA
n1hgE/Gx6226mmd3MN0E5jeom70zPYMSYe666K5Kc/UK5YCaBfxRagwSsotnZJlV
FfNmaowQkHEYCrdBKE6j2XnVwYH/+lYiGwMYwIDAQABAoIBAQDcmnke+rRP
ynHLPCquBpKmQc9YTB5ukXG6UQmM++H9ah61IHhD+5aEucG+Y3PfPM1agFo+J
XEGEkg+BqkDrBkGfP3YH+Ch5eEDXWW3GUo1kWpKqMxKUVtz+YGnErtIOKV
YMu9xhfiuObmsw66NGKr9pPoKmNSaDYyXkhLt5OXUOkFvy9LvaxA+m2mdCZp1
hIj1Ba64T0zgeOKbAKeAuwQQSG8UT+JWt8AK0AUnQHDC4HpdoH5yjyDAnYBJ
TbpIAOssZOwjDbpM8X2f14Y8dk/dXoRuTI3pBrXp0H9gC6LQRf/NiTxyixWxzHueG
fjALNQuIOmXKzygBN84en/4miiBAoGBAPihujOt39B7A83VYWkByUQl79PzJANv
F7jdFzcxKpmGC8TXBCQfdkuqdeSTg7J7RBV7c14MCcaUgPV18ucTW2puuityEjNSj
W2cufvhe0Cj+YlmDwCFFEZt15Gkgik0Zm6tuGaK6pS1gAIGaBtS3G9SDJMwNd378
Ewxw6XGGkXpAoGBAOkIbK9t2hyLWL2PkPkQn6gacXVq+DfeqAMxPOxvOPtXGi
WsJehos9ewjMoGXSHb7JUvmomI6XHinRa78+26q2D/fhvPnvs6KTx7psSRe/cjqfLlM
B9i12c1YG3MQeBgD33XOaeZqLFahaBbgNOOGf4mCnGbUCVEYV3QzSV9YbRrA
oGBAOTpahk4pc8540e4hOX8KgUfdI7M1kR/HPUsQbqj/te4jc9eM8baXLzPpZmco21
JhmbM8WwOY1W81nqobMqJjOoSJj/n14//Go1n9ehNMoBSOGZjW76byA4MBaRnN
Rugzgpq0VM/5TijXsb+hQ1bHe80OLWvdnj6A8TzMHHJUdk5AoGBAJbbJ1Dh8oLs
CoScviMeidzPUYfLueihMW7vnxsIXYEIQBsHOHsd3N7SojHesMfMkXl6mbZTdZy
OMVeYUS8i2vMuMrtaSvckDbHj8m/qJrA03D4r9F09JWjg+w3ZXwQb66txexdut/Ao
Q70tv1Y09cq7YaNuAhI+FDIhi8yrQGcFAoGBAPPDaFMxeBYNw+331NlNf1ybOsE
FgnyiZRsQipOOvTlO9HO5yVjIjM5BmbrJFDNyECjs4vnSAI2rGBaByPwxTQvSSu/L
VQ6XjIw/Yp7+6fkR5m6mHOPk9HS5ZUA2T5Kv55XL22nimzM9t7Us+mLNEJ7TQ
V1Z2i9GJPXqAu96+4UM
-----END RSA PRIVATE KEY-----

- Resultado do Manuel:

RSA key ok

-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAmukGuj/iVZ2P605vEIXcmwaFolQj7c3nHQIybO+rMm6Pk3S
EySIz6HUse0MWg4TFX5OEujHhLFxgAsWzyQcJGnQZkXMVIm6QxyKzeYdFTPD
cJ/3uGcrNAfJWWglxfWMiXKjqSgaCxYuDkj0dnPv3iFHGQbSeAmPY9bQVPtRFrA
G6xclUsfjtliiwtVJ6ARHNjBoUmRuUyJBS8qlEi6PNB4VjQTb/WAYXQy4p36POi+M
DwNIWTr/dYoPnD1PCSGOVD23BHFOXJsMgD/dLhpFbAzlEnboWC+Jk0foZkkUv3
eVF9AaCzmjhe6fT5x0gVC+RLhem+pdtXl2ep1E3PDn3ewIDAQABAoIBABU853A3
e/dS771J9o4kXBdg8IdN09MxjIL8nx8ySJ1UbRjBO8c7ijRPhDat/vMvC8RLvEGuvvlO
/NbEdh6UeVoIGs1HItmioPS8PDDoK8cdqoFNHgypMiwXJmGXs9iF89sSSXS2qc0dk
H9HI703CjvFQlIVyif3unINK3B+t8KaD36mpJ286CDpO0T+5cREULA1It7huNfpgE+
JCsQPEKhEFHh5EwCXT3BB97haNsf6araYpIP9aWhCA2gPyLQYf0y8d5VPzklzZ/X
6+pJ9xLHywpFPd+KR15HRHlD/amcylxdmjsnhioszc5AA8ag5JqBiamBHgSiUMRSB
+biEoQECgYEAyVCaqM/FgupFsi/hXIZBoRUssgvZa+tLXnWsfzsJv4cgJ3j7/vu5QH+
ZhaXd/PW+CKFV99ebflarkHSPtsVdzego8yHoRwMjyTCFtnOf845I8x8f7X6hP39nL+
mddpZ4lAPHallhHizmjibVVCBpWuzOOOmQC7OOJ0L59U2JXoECgYEAxP10jfTKi
qxNxt67FkQ/sUAkbdzRy5eYxZ4y7OMj/YIVfftNDT+ZkR0P7T3KvnaDRQCPmrNgR
0sdGVD3XZm5lEnkop6qAbjX6Z+uMokW3Z7zjT139menJJdrVWl3u16z419KHdRiJ9
zuCj853/FARpDOfnyPj3rZOGek8tMgz/sCgYAli9n8iBu/SfBLxnBSsFuHLorSfjFD1nO
NH4dXh2xPA2W01vSw3sPzSpkYexIG/tI9i9Gb0uOWUZXX8FVpcjAHmjgg+H7415
YSDPGzUKdRZoUmivSKd+adECbvobOTjYbZnEbSB+98EEXD12xML2tW4PmpVa
5e8FMf8XbrEFYBgQKBgGvhblprzBxjvniB9C1+lO8KdKjh/Ncln5niSHto7YXhHsoOv
STbRsutAdLoO0dRehRo+Tw8riZ9IWOC7uWI0ZQ/X4IbqHkm9L/SHkE4yJf4e+NG3
ZLJM0Ub08FD8Dlh5NxJjDqH3HV+TbK464YUBiJfHWcx6iEmox17zV7adybPAoGA
ThjIUzke7Ymp0U+gDLjLozzkTXK2Y7GpSkn6S1o+bkkVOQqF7epabDS8hyGZi44C
6WzEv7LxEykI+Yghjt0LCb3zYI6YFEZYu6KmOVnDHSGGaXH3InBF6N+bWnbwH
CRjbmwtQydbZY17sJxXuQcMNABnzSZUY6YOfm/KA59B/+o=
-----END RSA PRIVATE KEY-----

- Resultado do *usertest*:

-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAmiD1ZVF7ovTPSlvC+BW1lEjd92GMofebs7VB+itrJDALod2
221WM0PrOCfn7sk0GjRgALehpYPHAi8xRV3ft6VCASWOtOepIiSpZh7rMGL+jgzL
nvqu+XK872/1FRfJuFqQBbd5cEumJ028dr9xUfghZPJNvqKX8mCKkxHhkGBHvYv
w+2jQn6SbPDFmTfNBCnRibuA1p/0SFKBhMevfJLRR+bPV/uuzlCUDvC2dy8WtDo
WcBwficIOZoJCyii9wJqje5tyFAwrYcsseBD+dzJFckl2TddAZ6P63bJPvvA0iu7bfdXG
dEZ+/CtcXqcYJOOfA6hhtMTj9Up+CeEhqHeQIDAQABAoIBAHCnGFW2qdRgdMZ
XrXigfXhljf9LSHv1u9Ms741HgOcRSt9Da2yC6gqw1jnKgmI/FEO6QB9N2P/nkyFa9
DUnTjgTA8EgXrOO/vdqgcfIC3cnUv8JDQN7Cgc6eVkAlEpcuIRJ2VWRieC0220zsRI
hy4vW1EqHRLySnb4gzCdiC17fUpQMkNvVfQ65erKQGhwNPSqMpRa1WkvZ+MPc
khEeUI+B8XhP/DLwqlTUfEx4NiyrmyJzqhS+CumZQQK5RHfODaYXuM6xtiXN0++
agTn39KhTcKTp0SSarLyFKYCa82iMOmaDem6UneTEE3WRMoLHTrDASef+Wboy
vXIx3WAJHCUCgYEAyx9Wh1lQqBNVhZ3Ra6AzF7PMoMN581XhVuEWlVFdIrQ
Bz7qje73FoX386OE6aACxm6fTVIpqJnyfgIeJOcsF/RqMd+oqSjRkdgcrKzDzJjnR7I7s
xT4gOnzPmNzV7yB+mwEbzYrCKIA3Gx618NJhauheVCU4Xl/WKEe8GZOo2/cCgY
EAwkCKnxU9pKgddSt0tvYgQ3WF5Med8D1FCQnt+qnURlxp8fbwgUxjt75irboBgRE
4Vv3XvU/iIfN1Q4Yzg20zE2rP87DOz9KX3dk478ks0asb7K5dvGRq678z1+M737nq7
K07RpqF49y5CGvJH+HIxIjqixGRyZ0LvWfbtVYmfA8CgYAycSbY19pK0vpTAz0lg
BQQF8uCROj8/9/E5oLoM9twKcmlX5EHwrnYf+QVpREPENUKdaPqg7EWu64Uih
QO8RccosItaU51PQuRr/gNcst/O66hE2FDHkl8nNAlAvpxtt0Z+y1/Xq0Wx7hnmLnQA
z7EAM6kENYtwZj6Sc4xf9TYQwKBgQCsb+DeYVusTDSCK8ZbGFgBqlTmhzEz7x/
Wa0MfbhzrLOQ7kCtljCtFFDPC5kipi2DJEGOwQTaLTvR8sagO9iQOC5Z4TC76m4a
GwGrjqWEo6s1KKGs7bqTfi4b5EVW4P/FEkm75OPi8EtcKm6wZqjOwC56xPzJ8l/W
w+H44FjbpjwKBgQCDTsL/GNnebF3HYby41xAmCoNW2eE54O5MtoOuGE12CjZN
yR1HnduQeH9LFwzHud3Fkzk6NM7fSHDZXQ4xDBGpMioxAKmKFXgH/MUknXY
AjsE+bbSxfShwzz9I65P5Km4Zh8GssbZfGnGoP9a2iYfQZL39K8r2EnKFML54m70d
aA==
-----END RSA PRIVATE KEY-----

4- Gerar um ficheiro com um pedido de certificado

Objetivo: pedir um certificado

Comando: openssl req -new -key privkey.pem -out cert.csr

- Resultado do Hélder:

You are about to be asked to enter information that will be incorporated into your certificate request. What you are about to enter is what is called a Distinguished Name or a DN. There are quite a few fields, but you can leave some blank For some fields there will be a default value, If you enter '.', the field will be left blank.

Country Name (2 letter code) [AU]:PT
State or Province Name (full name) [Some-State]: Braga
Locality Name (eg, city) []: Guimaraes
Organization Name (eg, company) [Internet Widgits Pty Ltd]: Universidade do Minho
Organizational Unit Name (eg, section) []: Seguranca de Redes
Common Name (e.g. server FQDN or YOUR name) []: Grupo2
Email Address []: A75121@alunos.uminho.pt

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

A challenge password []: *12354*
An optional company name []:

- Resultado do Hugo:

You are about to be asked to enter information that will be incorporated into your certificate request. What you are about to enter is what is called a Distinguished Name or a DN. There are quite a few fields, but you can leave some blank. For some fields there will be a default value, If you enter '.', the field will be left blank.

Country Name (2 letter code) [AU]: PT
State or Province Name (full name) [Some-State]: Braga
Locality Name (eg, city) []: Guimaraes
Organization Name (eg, company) [Internet Widgits Pty Ltd]: Universidade do Minho
Organizational Unit Name (eg, section) []: Seguranca de Redes
Common Name (e.g. server FQDN or YOUR name) []: Grupo2
Email Address []: A48319@alunos.uminho.pt

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

A challenge password []: HP12354
An optional company name []:

- Resultado do Manuel:

You are about to be asked to enter information that will be incorporated into your certificate request. What you are about to enter is what is called a Distinguished Name or a DN. There are quite a few fields, but you can leave some blank For some fields there will be a default value, If you enter '.', the field will be left blank.

Country Name (2 letter code) [AU]: PT
State or Province Name (full name) [Some-State]: Braga
Locality Name (eg, city) []: Guimaraes
Organization Name (eg, company) [Internet Widgits Pty Ltd]: Universidade do Minho
Organizational Unit Name (eg, section) []: Segurança de Redes
Common Name (e.g. server FQDN or YOUR name) []: Grupo2
Email Address []: A76569@alunos.uminho.pt

Please enter the following 'extra' attributes to be sent with your certificate request:
A challenge password []: MC12354
An optional company name []:

- Resultado do *usertest*.

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) []: UM
Common Name (e.g. server FQDN or YOUR name) []: Teste Grupo2
Email Address []: manelcoutinho16@hotmail.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:12354
An optional company name []: Grupo2

Objetivo: verificar o estado do ficheiro de pedido do certificado

Comando: openssl req -text -noout -verify -in cert.csr

- Resultado do Hélder:

```
verify OK
Certificate Request:
    Data:
        Version: 0 (0x0)
        Subject: C=PT, ST=Braga, L=Guimaraes, O=Universidade do Minho, OU=Seguranca de Redes, CN=Grupo2/emailAddress=A75121@alunos.uminho.pt
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:9a:78:f5:f0:55:1d:27:70:42:95:1d:3c:1e:28:
                    97:ba:6a:c8:2a:27:1d:fe:c0:9d:fa:d1:89:3a:53:
                    7b:9a:98:44:77:4c:32:99:7b:c2:e5:e4:77:d8:14:
                    8f:06:3c:55:c9:7b:2b:8e:fd:21:43:77:8e:49:6f:
                    24:0d:ca:a2:bb:37:31:65:85:26:eb:54:fd:7d:cc:
                    c0:3e:fc:3b:61:5f:ac:43:39:b7:e2:2a:ae:89:1d:
                    c5:18:0c:31:d4:e9:b9:eb:41:af:f6:c5:1a:09:2c:
                    0f:d5:7b:ff:1f:0d:b9:c5:74:55:95:6f:28:f8:64:
                    77:ca:8f:21:16:b4:d5:bf:d0:24:b5:90:4d:dd:98:
                    13:dd:de:1d:41:f3:d9:68:96:83:12:90:70:c4:b9:
                    a6:dd:44:eb:31:3f:11:b7:55:01:e0:49:63:a2:73:
                    8b:a5:eb:21:03:15:be:fc:a4:30:bb:3c:95:1a:a5:
                    26:48:ca:40:6d:c9:27:7f:35:58:ac:94:34:e3:4c:
                    57:d3:0f:e9:95:04:fd:cc:51:1b:66:f4:c4:de:c6:
                    d4:75:75:e1:18:70:ab:f7:7c:60:12:1c:85:94:fb:
                    4f:58:31:99:eb:f3:97:b2:48:6f:67:e3:0f:24:c8:
                    12:d5:04:c9:89:52:59:ba:ae:0e:da:c3:64:17:ee:
                    74:0d
                Exponent: 65537 (0x10001)
        Attributes:
            challengePassword        :unable to print attribute
    Signature Algorithm: sha256WithRSAEncryption
        96:63:ba:44:c1:39:15:cb:3c:9a:cd:08:68:97:5b:43:4c:25:
        51:4e:7d:73:48:4d:fc:21:e8:c4:41:2b:05:67:ce:bd:00:bb:
        b5:2e:58:76:c2:54:95:9f:e3:00:62:4f:c4:e0:a1:01:fd:46:
        fd:aa:2c:8c:fa:ed:25:24:33:c6:8d:74:86:e1:e7:62:c6:29:
```

```
97:62:ec:2d:f2:57:d5:bd:e0:8d:e1:e5:b9:ed:a1:e1:df:a2:
e4:bc:67:f6:83:85:08:cf:ce:dd:96:e9:53:68:ed:44:3d:2d:
5c:ff:91:74:4c:da:9e:d3:8e:4d:9e:5d:50:3f:9f:46:ed:f6:
b9:65:16:23:58:db:43:03:f3:89:05:3d:8b:f9:98:fa:c5:34:
d2:98:f7:b4:a7:06:28:5e:53:16:73:4d:d7:65:a7:d2:88:c5:
50:3d:4c:2c:32:76:45:a8:df:08:08:10:b8:be:86:f4:fa:46:
6b:04:5f:86:98:8b:e0:6d:dc:aa:19:31:61:d3:63:87:c3:25:
23:41:5c:32:d0:ed:8e:27:90:33:9d:fd:a0:22:c4:07:58:e6:
b2:d5:61:8f:f9:3b:33:82:31:8c:15:13:21:bf:75:d2:b6:63:
9b:3e:25:64:a4:d5:d8:30:78:a2:a7:bc:77:65:8a:b7:3c:9f:
7e:1a:00:db
```

- Resultado do Hugo:

```
verify OK
Certificate Request:
    Data:
        Version: 0 (0x0)
        Subject: C=PT, ST=Braga, L=Guimaraes, O=Universidade do Minho,
OU=Seguranca de Redes, CN=Grupo2/emailAddress=A48319@alunos.uminho.pt
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:e2:53:61:15:76:aa:ec:26:59:a9:af:9d:ef:d8:
                    c2:d9:41:d7:84:3a:d3:41:3d:e8:c5:80:5a:25:25:
                    bb:0b:3c:cd:70:2c:cf:41:21:29:01:92:71:c8:2c:
                    0f:45:7a:1a:72:61:9c:28:a6:a5:27:dd:2d:0b:b2:
                    92:2b:e0:f3:dc:0d:7b:8c:51:67:56:3c:59:4a:da:
                    9f:4a:eb:a5:a6:68:11:0a:4d:bd:d7:25:5f:87:48:
                    0f:c6:a1:45:95:10:2e:3b:eb:e5:99:af:91:ec:21:
                    e3:1b:97:d9:98:58:b5:ef:33:4b:7f:f6:a2:9e:d5:
                    9c:71:1a:4c:9f:a0:69:62:d9:59:20:fc:de:06:13:
                    e2:9c:ac:89:0e:44:e7:5f:d4:bc:22:af:d9:4f:39:
                    f8:df:ce:4d:5e:34:16:ce:da:ac:06:44:67:15:bd:
                    2a:da:eb:8d:42:a5:21:67:ca:6b:63:9a:32:90:3b:
                    41:02:7d:61:80:4f:c6:c7:ad:b6:ea:69:9d:dc:c3:
                    74:13:98:de:a2:6e:f4:cc:f6:0c:49:87:ba:eb:a2:
                    b9:29:cf:d4:2b:96:02:68:17:f1:45:a8:30:4a:ca:
                    2d:9d:92:65:54:57:cd:99:aa:30:42:41:c4:60:2a:
                    dd:04:a1:3a:8f:65:e7:57:06:07:ff:e9:58:88:6c:
                    0c:63
                Exponent: 65537 (0x10001)
        Attributes:
            challengePassword        :unable to print attribute
    Signature Algorithm: sha256WithRSAEncryption
        80:f0:31:9b:f8:21:ac:c1:cd:3f:96:00:a2:46:c6:a3:29:08:
        a2:f6:91:33:bb:1b:f4:f4:ca:e1:91:3b:be:39:51:a8:04:4a:
        9b:91:05:28:d1:65:b7:5d:fd:6d:c5:9e:17:0b:21:0a:33:6c:
        e8:b6:4b:6a:eb:2a:0a:c8:0f:bd:a2:47:9c:ab:62:ab:2f:28:
```

```
        05:38:c8:d5:80:bb:d6:9c:10:16:a8:80:0a:e2:f8:61:44:0c:
        c1:d9:bf:77:0a:58:83:90:89:42:36:12:db:e4:77:e5:f6:0a:
        fe:d9:66:5e:e0:96:7c:bc:ad:b2:34:ee:4f:60:55:0c:40:f9:
        95:0e:5f:2f:db:90:37:57:32:d4:ff:95:64:90:a0:1a:f9:42:
        cd:a6:2c:f6:0a:22:38:16:7a:83:eb:24:4a:a3:10:1d:44:ef:
        73:50:d3:aa:af:e2:46:72:af:e0:f5:be:1f:e7:10:73:12:35:
        34:87:df:53:24:be:26:1f:5c:20:25:8e:bc:18:89:cf:81:7f:
        1b:4d:0f:cb:c0:96:89:be:d7:05:36:36:b7:01:51:56:32:8a:
        b6:3d:ff:f4:c3:7f:e8:3f:2e:25:43:ca:9a:d7:74:9c:96:b2:
        58:d2:85:6f:da:b2:69:96:38:f5:d2:dd:58:fd:25:64:40:15:
        a9:51:12:72
```

- Resultado do Manuel:

```
verify OK
Certificate Request:
    Data:
        Version: 0 (0x0)
        Subject: C=PT, ST=Braga, L=Guimaraes, O=Universidade do Minho,
OU=Seguran\xC3\x83\xC2\xA7a de Redes,
CN=Grupo2/emailAddress=A76569@alunos.uminho.pt
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:9a:e9:06:ba:3f:e2:55:9d:8f:eb:4e:6f:10:85:
                    dc:9b:06:85:a2:54:23:ed:cd:e7:1d:02:32:6c:ef:
                    ab:32:6e:8f:93:74:84:c9:22:33:e8:75:2c:7b:43:
                    16:83:84:c5:5f:93:84:ba:31:e1:2c:5c:60:02:c5:
                    b3:c9:07:09:1a:74:19:91:73:15:22:6e:90:c7:22:
                    b3:79:87:45:4c:f0:dc:27:fd:ee:19:ca:cd:01:f2:
                    56:5a:09:71:7d:63:22:5c:a8:ea:4a:06:82:c5:8b:
                    83:92:3d:1d:9c:fb:f7:88:51:c6:41:b4:9e:02:63:
                    d8:f5:b4:15:3e:d4:45:ac:01:ba:c5:c9:54:b1:f8:
                    ed:96:28:b0:b5:52:7a:01:11:cd:8c:1a:14:99:1b:
                    94:c8:90:52:f2:a9:44:8b:a3:cd:07:85:63:41:36:
                    ff:58:06:17:43:2e:29:df:a3:ce:8b:e3:03:c0:d2:
                    16:4e:bf:dd:62:83:e7:0f:53:c2:48:63:95:0f:6d:
                    c1:1c:53:97:26:c3:20:0f:f7:4b:86:91:5b:03:39:
                    44:9d:ba:16:0b:e2:64:d1:fa:19:92:45:2f:dd:e5:
                    45:f4:06:82:ce:68:e1:7b:a7:d3:e7:1d:20:54:2f:
                    91:2e:17:a6:fa:97:6d:5e:5d:9e:a7:51:37:3c:39:
                    f7:7b
                Exponent: 65537 (0x10001)
        Attributes:
            challengePassword        :unable to print attribute
    Signature Algorithm: sha256WithRSAEncryption
        6c:b5:cd:e3:b1:4d:ca:86:3e:eb:0a:78:e0:6d:a2:d0:14:9b:
        19:79:e9:ce:8a:49:f2:e7:1b:03:67:7b:b4:02:c4:5d:a6:6a:
        5c:45:d3:1e:b6:76:58:cb:e8:d1:2b:d6:28:48:51:7c:9f:b3:
```

```
        e8:8d:cb:82:b1:3e:ac:7e:f7:23:a3:54:aa:93:46:1f:df:3d:
        d4:db:cd:78:89:c1:10:b8:fa:5b:cd:28:db:54:83:eb:6d:21:
        5c:09:7f:28:bd:6d:eb:c5:d7:86:2c:f4:c6:57:3f:ff:a9:07:
        bf:db:15:a4:20:5b:80:df:03:68:11:77:18:d5:23:14:aa:b7:
        81:32:cf:c4:84:5f:29:e0:05:d9:90:aa:bc:6e:62:50:a1:65:
        55:63:48:d7:70:60:32:a3:11:43:f4:8c:61:01:6f:6e:48:c7:
        30:f6:73:5d:55:21:c7:0f:cb:ec:91:17:1b:7d:f7:6f:d3:24:
        c2:85:9e:43:44:8c:19:3f:bf:2c:2e:f2:59:da:38:aa:26:4a:
        f5:6c:9e:cc:30:0b:25:e0:a9:69:58:97:c6:a2:76:09:97:bb:
        1b:bf:45:de:61:51:25:1e:1b:f8:ef:75:8a:c3:d4:8a:57:89:
        42:21:81:71:0a:84:10:7d:69:99:ca:61:e4:fe:cf:36:a5:d0:
        cb:fa:9b:5d
```

- Resultado do *usertest*

```
verify OK
Certificate Request:
    Data:
        Version: 0 (0x0)
        Subject: C=PT, ST=Braga, L=Braga, O=UMinho, OU=UM, CN=Teste
Grupo2/emailAddress=manelcoutinho16@hotmail.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:9a:20:f5:65:51:7b:a2:f4:cf:4a:5b:c2:f8:15:
                    b5:94:48:dd:f7:61:8c:a1:f7:9b:b3:b5:41:fa:2b:
                    6b:24:30:0b:a1:dd:b6:db:55:8c:d0:fa:ce:09:f9:
                    fb:b2:4d:06:8d:18:00:2d:e8:69:60:f1:c0:8b:cc:
                    51:57:77:ed:e9:50:80:49:63:ad:39:ea:48:89:2a:
                    59:87:ba:cc:18:bf:a3:83:32:e7:be:ab:be:5c:af:
                    3b:db:fd:45:45:f2:6e:16:a4:01:6d:de:5c:12:e9:
                    89:d3:6f:1d:af:dc:54:7e:08:59:3c:93:6f:a8:a5:
                    fc:98:22:a4:c4:78:64:18:11:ef:62:fc:3e:da:34:
                    27:e9:26:cf:0c:59:93:7c:d0:42:9d:18:9b:b8:0d:
                    69:ff:44:85:28:18:4c:7a:f7:c9:2d:14:7e:6c:f5:
                    7f:ba:ec:e5:09:40:ef:0b:67:72:f1:6b:43:a1:67:
                    01:c1:f8:9c:20:e6:68:24:2c:a2:8b:dc:09:aa:37:
                    b9:b7:21:40:c2:b6:1c:b2:c7:81:0f:e7:73:24:57:
                    24:97:64:dd:74:06:7a:3f:ad:db:24:fb:ef:03:48:
                    ae:ed:b7:dd:5c:67:44:67:ef:c2:b5:c5:ea:71:82:
                    4e:39:f0:3a:86:1b:4c:4e:3f:54:a7:e0:9e:12:1a:
                    87:79
                Exponent: 65537 (0x10001)
        Attributes:
            challengePassword        :unable to print attribute
            unstructuredName         :unable to print attribute
    Signature Algorithm: sha256WithRSAEncryption
        26:d1:2c:5d:d2:40:f3:d5:34:32:97:b8:fb:ef:c1:f5:fa:5b:
        1e:c2:e4:7e:6c:53:f4:85:66:c6:3b:2e:85:23:27:ad:eb:a7:
```

82:7d:fe:68:4e:22:ce:4c:5a:e6:c0:e6:39:e0:e8:d8:22:09:
c2:27:09:aa:9d:a6:3d:18:e7:ae:50:25:fb:4f:63:bb:f2:c3:
90:4f:82:64:f8:4c:c9:61:19:0f:03:b0:14:78:f2:47:b9:91:
0e:b3:f3:17:d1:19:05:4f:7d:53:21:a3:e7:10:a4:6e:13:4d:
14:d8:23:63:51:60:2f:7a:67:32:99:e5:98:97:a8:fe:3a:ff:
7e:69:cc:83:a7:75:df:cf:ba:29:8c:4d:24:c0:92:87:4e:54:
0d:7a:eb:ce:5a:8a:c7:cd:78:41:92:30:32:28:56:43:f9:9a:
c1:f4:73:2e:37:2a:89:36:19:9c:39:12:ef:11:72:f5:b2:fe:
51:e8:03:b9:98:d9:58:d9:7c:b0:61:37:e3:9e:60:6c:b9:28:
b8:03:ae:d7:6e:08:1a:b0:5e:2c:1a:54:20:eb:18:c0:d9:11:
bc:a0:e9:90:44:29:95:9a:45:70:f8:0a:f6:00:1e:de:15:7f:
73:33:77:47:df:c3:ca:ec:e1:eb:a1:40:3a:f1:47:0e:a8:eb:
fc:cd:a8:17

5- Gerar um certificado auto assinado (X509)

Objetivo: gerar certificado X509 auto-assinado.

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

- Resultado do Hélder:

Signature ok
subject=/C=PT/ST=Braga/L=Guimaraes/O=Universidade do Minho/OU=Seguranca de Redes/CN=Grupo2/emailAddress=A75121@alunos.uminho.pt
Getting Private key

- Resultado do Hugo:

Signature ok
subject=/C=PT/ST=Braga/L=Guimaraes/O=Universidade do Minho/OU=Seguranca de Redes/CN=Grupo2/emailAddress=A48319@alunos.uminho.pt
Getting Private key

- <u>Resultado do Manuel:</u>

Signature ok
subject=/C=PT/ST=Braga/L=Guimaraes/O=Universidade do Minho/OU=Seguranca de Redes/CN=Grupo2/emailAddress=A76569@alunos.uminho.pt
Getting Private key

- Resultado do *usertest.*

Signature ok
subject=/C=PT/ST=Braga/L=Braga/O=UMinho/OU=UM/CN=Teste Grupo2/emailAddress=manelcoutinho16@hotmail.com
Getting Private key

6- Criação da Autoridade de Certificação

Na Figura 3 temos os primeiros parâmetros para a criação dos CA, onde podemos ver a imagem com as opções selecionadas para gerar o par de chaves do grupo 2.

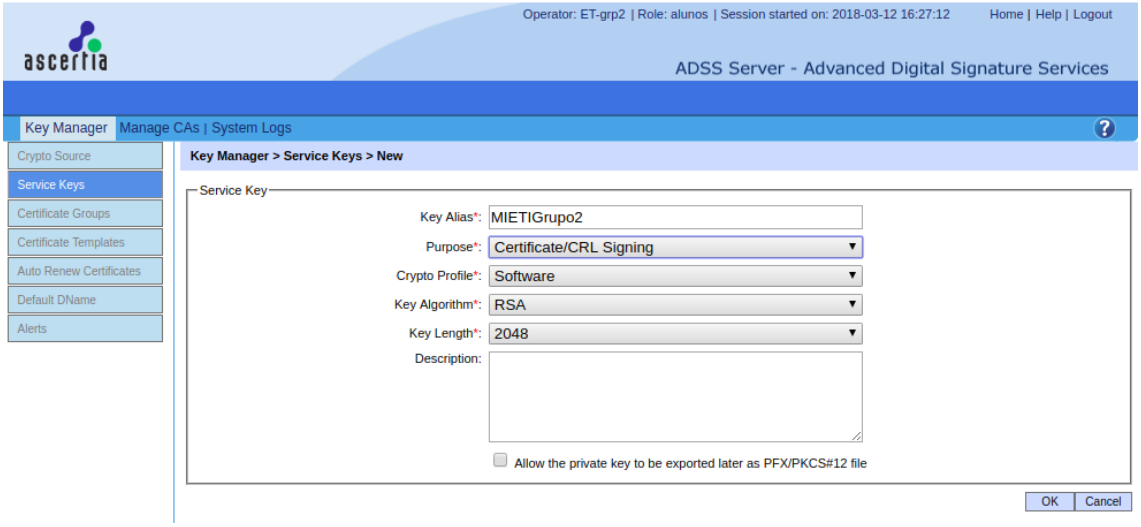


Figura 3 – Criação do novo par de chaves.

7- Configuração da CA

Na Figura 4, estão os parâmetros utilizados na criação do certificado do Grupo2.

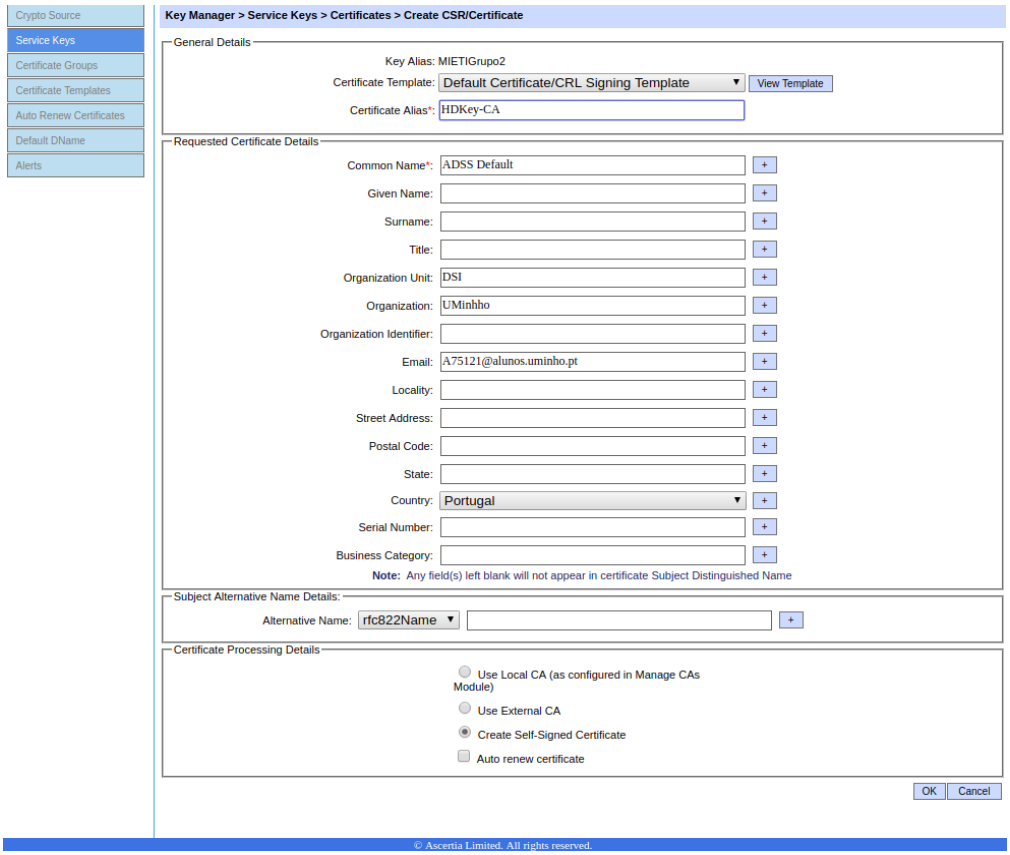
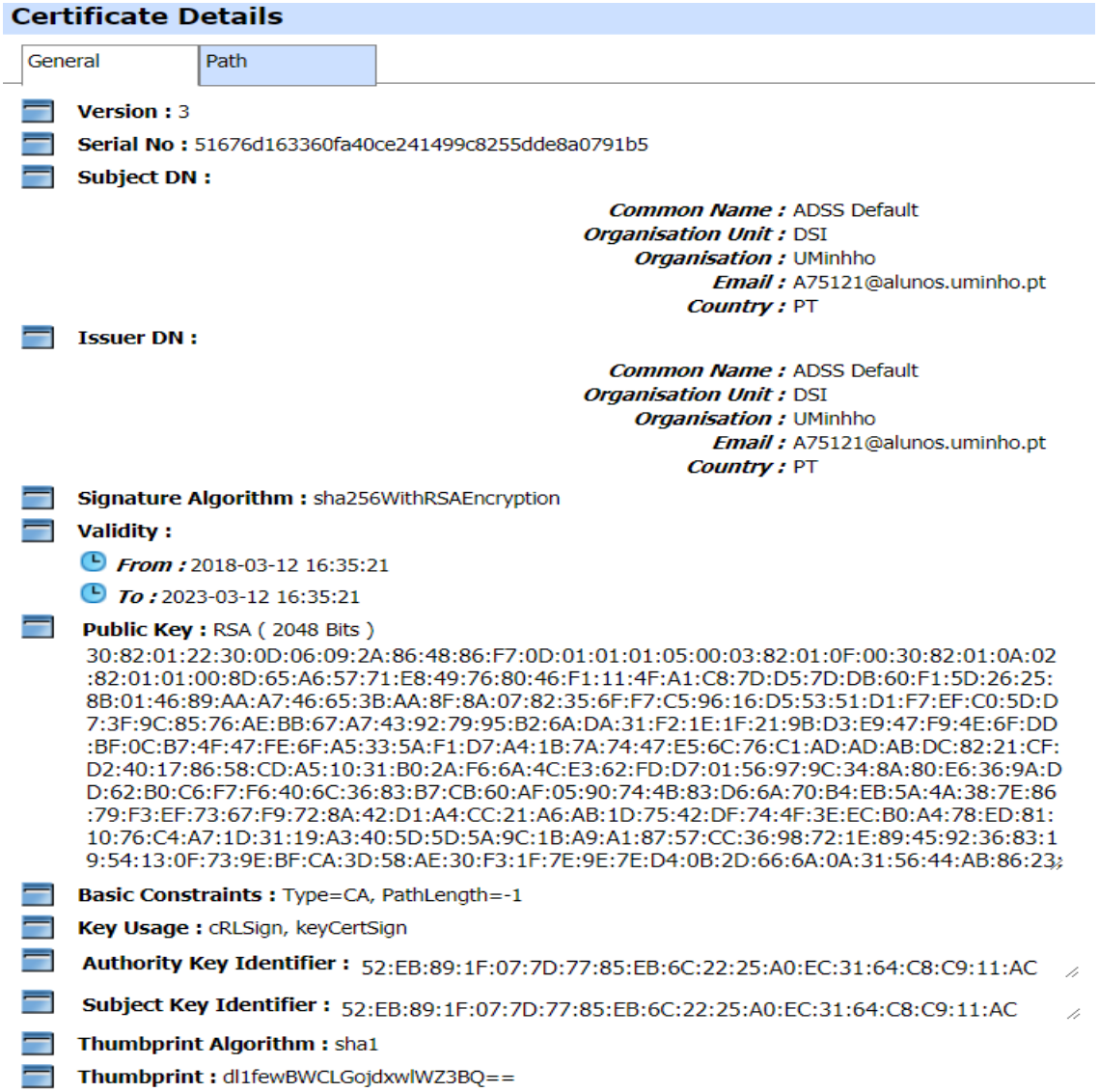


Figura 4 – Criação do certificado do Grupo2.

8- Detalhes do certificado

Na Figura 5 são apresentadas as características do certificado.



Certificate Details

General | Path

Version : 3

Serial No : 51676d163360fa40ce241499c8255dde8a0791b5

Subject DN :

Common Name : ADSS Default
Organisation Unit : DSI
Organisation : UMinhho
Email : A75121@alunos.uminho.pt
Country : PT

Issuer DN :

Common Name : ADSS Default
Organisation Unit : DSI
Organisation : UMinhho
Email : A75121@alunos.uminho.pt
Country : PT

Signature Algorithm : sha256WithRSAEncryption

Validity :

From : 2018-03-12 16:35:21

To : 2023-03-12 16:35:21

Public Key : RSA (2048 Bits)

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02
:82:01:01:00:8D:65:A6:57:71:E8:49:76:80:46:F1:11:4F:A1:C8:7D:D5:7D:DB:60:F1:5D:26:25:
8B:01:46:89:AA:A7:46:65:3B:AA:8F:8A:07:82:35:6F:F7:C5:96:16:D5:53:51:D1:F7:EF:C0:5D:D
7:3F:9C:85:76:AE:BB:67:A7:43:92:79:95:B2:6A:DA:31:F2:1E:1F:21:9B:D3:E9:47:F9:4E:6F:DD
:BF:0C:B7:4F:47:FE:6F:A5:33:5A:F1:D7:A4:1B:7A:74:47:E5:6C:76:C1:AD:AD:AB:DC:82:21:CF:
D2:40:17:86:58:CD:A5:10:31:B0:2A:F6:6A:4C:E3:62:FD:D7:01:56:97:9C:34:8A:80:E6:36:9A:D
D:62:B0:C6:F7:F6:40:6C:36:83:B7:CB:60:AF:05:90:74:4B:83:D6:6A:70:B4:EB:5A:4A:38:7E:86
:79:F3:EF:73:67:F9:72:8A:42:D1:A4:CC:21:A6:AB:1D:75:42:DF:74:4F:3E:EC:B0:A4:78:ED:81:
10:76:C4:A7:1D:31:19:A3:40:5D:5D:5A:9C:1B:A9:A1:87:57:CC:36:98:72:1E:89:45:92:36:83:1
9:54:13:0F:73:9E:BF:CA:3D:58:AE:30:F3:1F:7E:9E:7E:D4:0B:2D:66:6A:0A:31:56:44:AB:86:23

Basic Constraints : Type=CA, PathLength=-1

Key Usage : cRLSign, keyCertSign

Authority Key Identifier : 52:EB:89:1F:07:7D:77:85:EB:6C:22:25:A0:EC:31:64:C8:C9:11:AC

Subject Key Identifier : 52:EB:89:1F:07:7D:77:85:EB:6C:22:25:A0:EC:31:64:C8:C9:11:AC

Thumbprint Algorithm : sha1

Thumbprint : dl1fewBWCLGojdxwlWZ3BQ==

Figura 5 - Detalhes do certificado.

9- Configuração da CA

Na figura 6 temos os restantes parâmetros necessários à criação da nossa CA entre os quais especificamos que o tempo de espera para a publicação da nossa CRL será de dois minutos.

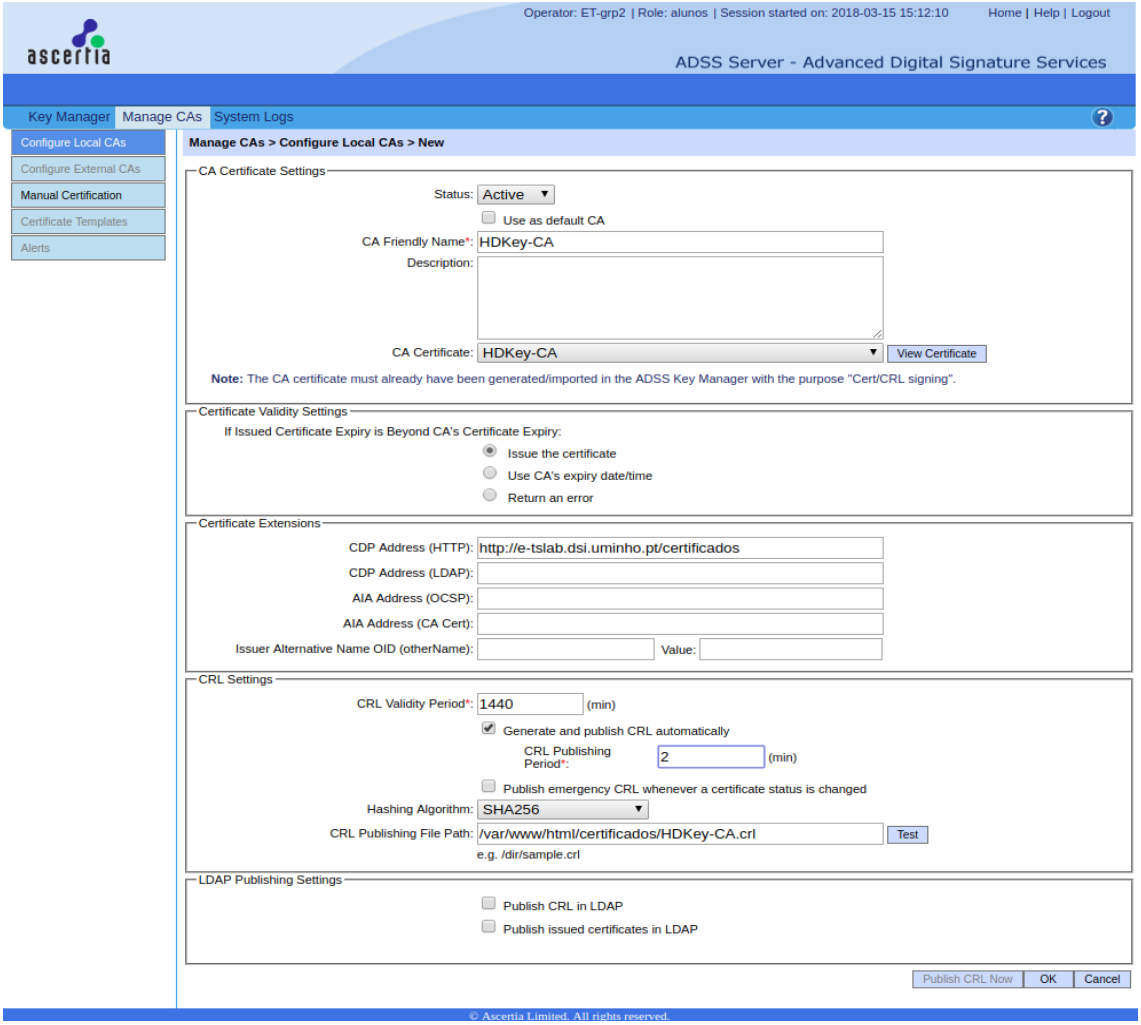


Figura 6 - Configuração da CA.

10- Assinar os pedidos de certificados individuais

Nas Figura 7, Figura 8, Figura 9 e Figura 10 podemos ver as assinaturas dos pedidos dos certificados individuais de forma a obter os certificados públicos de todos os elementos do grupo.

- Resultado do Hélder:

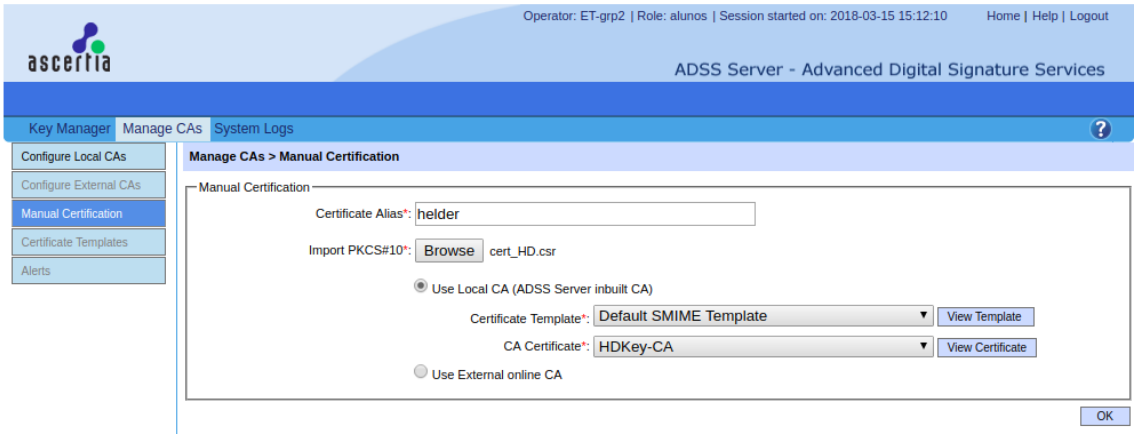


Figura 7 - Assinatura do certificado do Hélder.

- Resultado do Hugo:

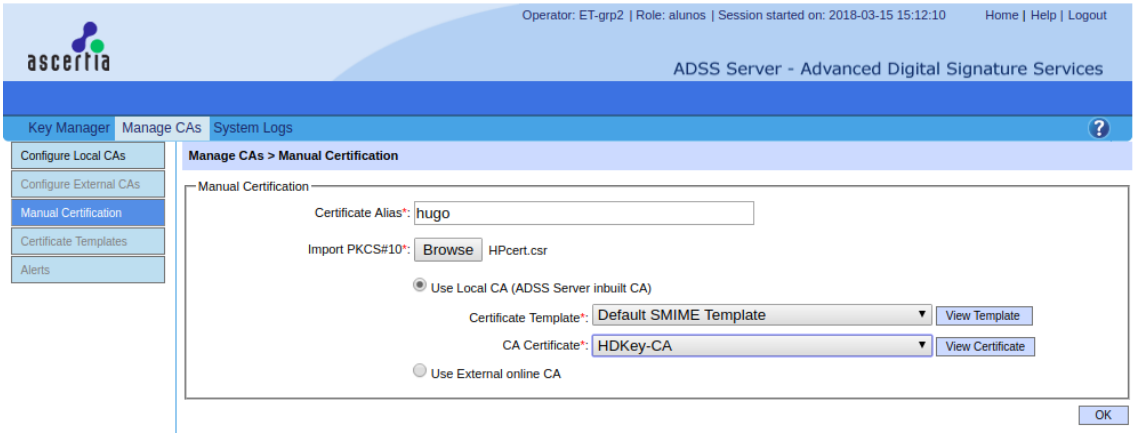


Figura 8 - Assinatura do certificado do Hugo.

- Resultado do Manuel:

Aproveitamos que na criação do certificado no Manuel obtivemos um erro. Erro esse que se deve ao campo *Certificate Alias* não admitir letras maiúsculas. Na Figura 9 podemos observar esse mesmo erro.

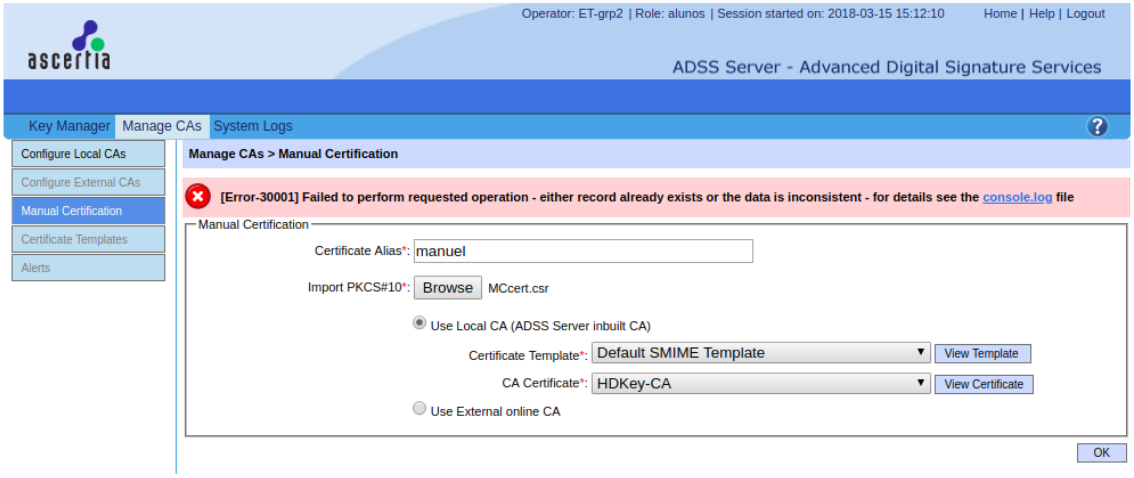


Figura 9 - Assinatura do certificado do Manuel.

- Resultado do usertest:

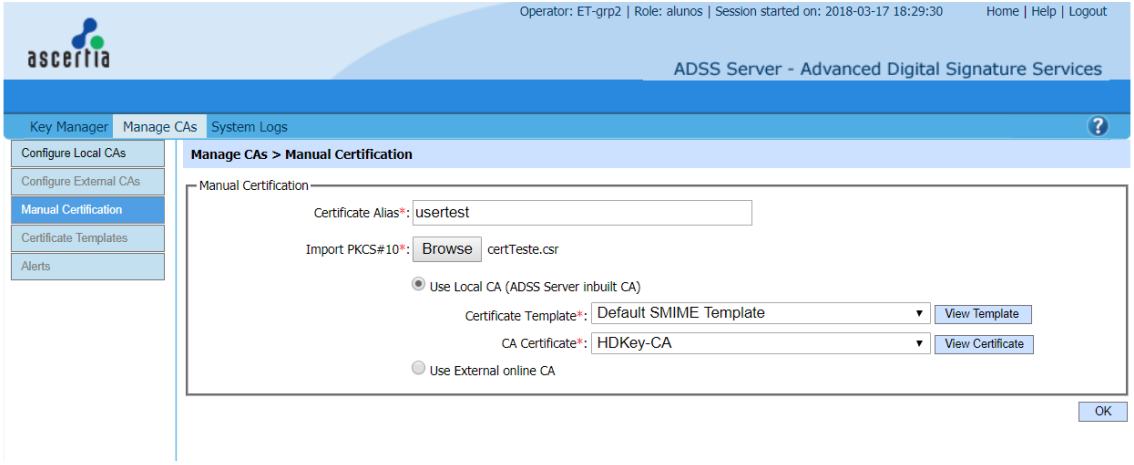


Figura 10 - Assinatura do certificado do usertest.

11- Verificação dos certificados individuais

Na Figura 11 temos todos os certificados emitidos para os elementos do grupo e mais um para teste.

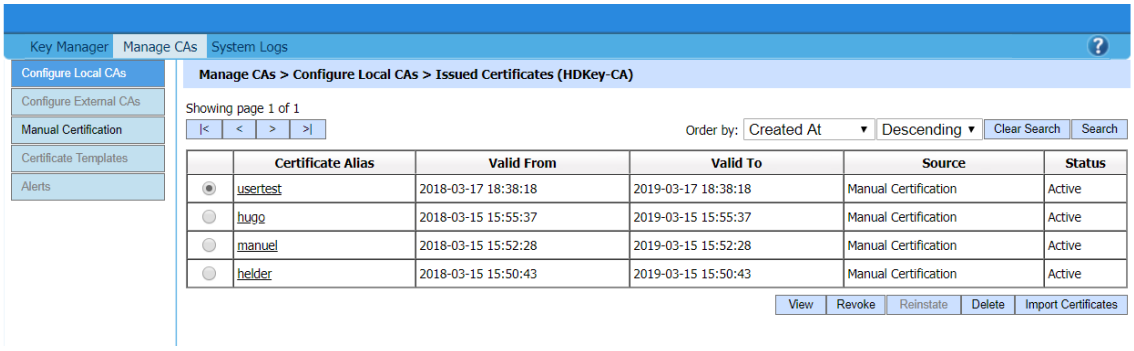


Figura 11 - Vista geral dos certificados individuais.

Foi nos também pedido para colocar no logbook o conteúdo de cada um dos certificados:

- Resultado do Hélder:

Version: 3
Serial No: 00de65a91e9a320f89ce433faf0676820b76c40875
Subject DN:
Email: A75121@alunos.uminho.pt
Common Name: Grupo2
Organisation Unit: Seguranca de Redes
Organisation: Universidade do Minho
Locality: Guimaraes
State: Braga
Country: PT
Issuer DN:
Common Name: ADSS Default
Organisation Unit: DSI
Organisation: UMinhho
Email: A75121@alunos.uminho.pt
Country: PT
Signature Algorithm: sha256WithRSAEncryption
Validity:
From: 2018-03-15 15:50:43
To: 2019-03-15 15:50:43
Public Key: RSA (2048 Bits)

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:
0A:02:82:01:01:00:9A:78:F5:F0:55:1D:27:70:42:95:1D:3C:1E:28:97:BA:6A:C8:2A:27
:1D:FE:C0:9D:FA:D1:89:3A:53:7B:9A:98:44:77:4C:32:99:7B:C2:E5:E4:77:D8:14:8F:
06:3C:55:C9:7B:2B:8E:FD:21:43:77:8E:49:6F:24:0D:CA:A2:BB:37:31:65:85:26:EB:5
4:FD:7D:CC:C0:3E:FC:3B:61:5F:AC:43:39:B7:E2:2A:AE:89:1D:C5:18:0C:31:D4:E9:
B9:EB:41:AF:F6:C5:1A:09:2C:0F:D5:7B:FF:1F:0D:B9:C5:74:55:95:6F:28:F8:64:77:C
A:8F:21:16:B4:D5:BF:D0:24:B5:90:4D:DD:98:13:DD:DE:1D:41:F3:D9:68:96:83:12:9

0:70:C4:B9:A6:DD:44:EB:31:3F:11:B7:55:01:E0:49:63:A2:73:8B:A5:EB:21:03:15:BE
:FC:A4:30:BB:3C:95:1A:A5:26:48:CA:40:6D:C9:27:7F:35:58:AC:94:34:E3:4C:57:D3:
0F:E9:95:04:FD:CC:51:1B:66:F4:C4:DE:C6:D4:75:75:E1:18:70:AB:F7:7C:60:12:1C:8
5:94:FB:4F:58:31:99:EB:F3:97:B2:48:6F:67:E3:0F:24:C8:12:D5:04:C9:89:52:59:BA:A
E:0E:DA:C3:64:17:EE:74:0D:02:03:01:00:01

Basic Constraints: Type=End Entity
Key Usage: nonRepudiation, keyEncipherment, digitalSignature
Extended Key Usage: emailProtection

Authority Key Identifier:
52:EB:89:1F:07:7D:77:85:EB:6C:22:25:A0:EC:31:64:C8:C9:11:AC

Subject Key Identifier:
D5:35:2A:0F:46:10:B2:B2:1C:43:3F:8C:8B:DB:FF:6E:04:9C:17:4D
Thumbprint Algorithm: sha1
Thumbprin : talGK6RNl9qIRiDV5uqbAQ==

- Resultado do Hugo:

Version: 3
Serial No: 021e3203f0442f2bfe9b5de09643c30271213756
Subject DN:
    Email: A48319@alunos.uminho.pt
    Common Name: Grupo2
    Organisation Unit: Seguranca de Redes
    Organisation: Universidade do Minho
    Locality: Guimaraes
    State: Braga
    Country: PT
Issuer DN:
    Common Name: ADSS Default
    Organisation Unit: DSI
    Organisation: UMinhho
    Email: A75121@alunos.uminho.pt
    Country: PT
Signature Algorithm: sha256WithRSAEncryption
Validity:
    From: 2018-03-15 15:55:37
    To: 2019-03-15 15:55:37
Public Key: RSA (2048 Bits)

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:
0A:02:82:01:01:00:E2:53:61:15:76:AA:EC:26:59:A9:AF:9D:EF:D8:C2:D9:41:D7:84:3
A:D3:41:3D:E8:C5:80:5A:25:25:BB:0B:3C:CD:70:2C:CF:41:21:29:01:92:71:C8:2C:0
F:45:7A:1A:72:61:9C:28:A6:A5:27:DD:2D:0B:B2:92:2B:E0:F3:DC:0D:7B:8C:51:67:5
6:3C:59:4A:DA:9F:4A:EB:A5:A6:68:11:0A:4D:BD:D7:25:5F:87:48:0F:C6:A1:45:95:1
0:2E:3B:EB:E5:99:AF:91:EC:21:E3:1B:97:D9:98:58:B5:EF:33:4B:7F:F6:A2:9E:D5:9
C:71:1A:4C:9F:A0:69:62:D9:59:20:FC:DE:06:13:E2:9C:AC:89:0E:44:E7:5F:D4:BC:2

2:AF:D9:4F:39:F8:DF:CE:4D:5E:34:16:CE:DA:AC:06:44:67:15:BD:2A:DA:EB:8D:42
:A5:21:67:CA:6B:63:9A:32:90:3B:41:02:7D:61:80:4F:C6:C7:AD:B6:EA:69:9D:DC:C
3:74:13:98:DE:A2:6E:F4:CC:F6:0C:49:87:BA:EB:A2:B9:29:CF:D4:2B:96:02:68:17:F
1:45:A8:30:4A:CA:2D:9D:92:65:54:57:CD:99:AA:30:42:41:C4:60:2A:DD:04:A1:3A:8
F:65:E7:57:06:07:FF:E9:58:88:6C:0C:63:02:03:01:00:01

Basic Constraints: Type=End Entity
Key Usage: nonRepudiation, keyEncipherment, digitalSignature
Extended Key Usage: emailProtection

Authority Key Identifier:
52:EB:89:1F:07:7D:77:85:EB:6C:22:25:A0:EC:31:64:C8:C9:11:AC

Subject Key Identifier:
0E:58:FF:67:4B:00:EC:AE:D6:7A:53:BE:88:E2:04:84:CD:D9:5A:F6
Thumbprint Algorithm: sha1
Thumbprint: D0AmkPlnwfVtUmjpkUKGrQ==

- Resultado do Manuel:

Version: 3
Serial No: 772d018f03669407d4deb396010ab5f552cc1d90
Subject DN:
    Email: A76569@alunos.uminho.pt
    Common Name: Grupo2
    Organisation Unit: Segurança de Redes
    Organisation: Universidade do Minho
    Locality: Guimaraes
    State: Braga
    Country: PT
Issuer DN:
    Common Name: ADSS Default
    Organisation Unit: DSI
    Organisation: UMinhho
    Email: A75121@alunos.uminho.pt
    Country: PT
Signature Algorithm: sha256WithRSAEncryption
Validity:
    From: 2018-03-15 15:52:28
    To: 2019-03-15 15:52:28
Public Key: RSA (2048 Bits)

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:
0A:02:82:01:01:00:9A:E9:06:BA:3F:E2:55:9D:8F:EB:4E:6F:10:85:DC:9B:06:85:A2:5
4:23:ED:CD:E7:1D:02:32:6C:EF:AB:32:6E:8F:93:74:84:C9:22:33:E8:75:2C:7B:43:16:
83:84:C5:5F:93:84:BA:31:E1:2C:5C:60:02:C5:B3:C9:07:09:1A:74:19:91:73:15:22:6E:
90:C7:22:B3:79:87:45:4C:F0:DC:27:FD:EE:19:CA:CD:01:F2:56:5A:09:71:7D:63:22:5
C:A8:EA:4A:06:82:C5:8B:83:92:3D:1D:9C:FB:F7:88:51:C6:41:B4:9E:02:63:D8:F5:B
4:15:3E:D4:45:AC:01:BA:C5:C9:54:B1:F8:ED:96:28:B0:B5:52:7A:01:11:CD:8C:1A:1

4:99:1B:94:C8:90:52:F2:A9:44:8B:A3:CD:07:85:63:41:36:FF:58:06:17:43:2E:29:DF:A
3:CE:8B:E3:03:C0:D2:16:4E:BF:DD:62:83:E7:0F:53:C2:48:63:95:0F:6D:C1:1C:53:97:
26:C3:20:0F:F7:4B:86:91:5B:03:39:44:9D:BA:16:0B:E2:64:D1:FA:19:92:45:2F:DD:E
5:45:F4:06:82:CE:68:E1:7B:A7:D3:E7:1D:20:54:2F:91:2E:17:A6:FA:97:6D:5E:5D:9E
:A7:51:37:3C:39:F7:7B:02:03:01:00:01
Basic Constraints: Type=End Entity
Key Usage: nonRepudiation, keyEncipherment, digitalSignature
Extended Key Usage: emailProtection

Authority Key Identifier:
52:EB:89:1F:07:7D:77:85:EB:6C:22:25:A0:EC:31:64:C8:C9:11:AC

Subject Key Identifier:
7E:81:BC:48:B9:C3:F7:60:EC:11:F0:82:5E:A9:69:41:F9:64:A1:BD
Thumbprint Algorithm: sha1
Thumbprint: aCKRlshWa1ghXUiP2+RgJw==

- Resultado do usertest:

Version: 3
Serial No: 00d1279f435e9c8fb133e00bdf090f8b4a24d00331
Subject DN:
Email: manelcoutinho16@hotmail.com
Common Name: Teste Grupo2
Organisation Unit: UM
Organisation: UMinho
Locality: Braga
State: Braga
Country: PT
Issuer DN:
Common Name: ADSS Default
Organisation Unit: DSI
Organisation: UMinhho
Email: A75121@alunos.uminho.pt
Country: PT
Signature Algorithm: sha256WithRSAEncryption
Validity:
From: 2018-03-17 18:38:18
To: 2019-03-17 18:38:18
Public Key: RSA (2048 Bits)

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:
0A:02:82:01:01:00:9A:20:F5:65:51:7B:A2:F4:CF:4A:5B:C2:F8:15:B5:94:48:DD:F7:61
:8C:A1:F7:9B:B3:B5:41:FA:2B:6B:24:30:0B:A1:DD:B6:DB:55:8C:D0:FA:CE:09:F9:
FB:B2:4D:06:8D:18:00:2D:E8:69:60:F1:C0:8B:CC:51:57:77:ED:E9:50:80:49:63:AD:3
9:EA:48:89:2A:59:87:BA:CC:18:BF:A3:83:32:E7:BE:AB:BE:5C:AF:3B:DB:FD:45:45
:F2:6E:16:A4:01:6D:DE:5C:12:E9:89:D3:6F:1D:AF:DC:54:7E:08:59:3C:93:6F:A8:A5:
FC:98:22:A4:C4:78:64:18:11:EF:62:FC:3E:DA:34:27:E9:26:CF:0C:59:93:7C:D0:42:9
D:18:9B:B8:0D:69:FF:44:85:28:18:4C:7A:F7:C9:2D:14:7E:6C:F5:7F:BA:EC:E5:09:40
:EF:0B:67:72:F1:6B:43:A1:67:01:C1:F8:9C:20:E6:68:24:2C:A2:8B:DC:09:AA:37:B9:

B7:21:40:C2:B6:1C:B2:C7:81:0F:E7:73:24:57:24:97:64:DD:74:06:7A:3F:AD:DB:24:F
B:EF:03:48:AE:ED:B7:DD:5C:67:44:67:EF:C2:B5:C5:EA:71:82:4E:39:F0:3A:86:1B:4
C:4E:3F:54:A7:E0:9E:12:1A:87:79:02:03:01:00:01
Basic Constraints: Type=End Entity
Key Usage: nonRepudiation, keyEncipherment, digitalSignature
Extended Key Usage: emailProtection

Authority Key Identifier:
52:EB:89:1F:07:7D:77:85:EB:6C:22:25:A0:EC:31:64:C8:C9:11:AC

Subject Key Identifier:
EF:AC:CA:2B:5F:26:63:9E:52:46:AF:59:3E:D7:36:2C:89:9C:3A:14
Thumbprint Algorithm: sha1
Thumbprint: 3cKnTMmWvaxjLo9PduSshA==

12- Gerar o ficheiro PKCS#12

Na Figura 12 temos os comandos introduzidos para criar o ficheiro PKCS#12.

```
manuel@manuel-X550CL:~/MEGAsync/Universidade/SRC/TP2/MC/12$ ls
certificate.cer  manel.cer  MCcert.csr  MCprivcert.crt
manuel@manuel-X550CL:~/MEGAsync/Universidade/SRC/TP2/MC/12$ openssl x509 -i
nform der -in manel.cer -out manelPubCert.pem
manuel@manuel-X550CL:~/MEGAsync/Universidade/SRC/TP2/MC/12$ openssl x509 -i
nform der -in certificate.cer -out CAcert.pem
manuel@manuel-X550CL:~/MEGAsync/Universidade/SRC/TP2/MC/12$ openssl pkcs12
-export -in manelPubCert.pem -inkey MCprivkey.pem -certfile CAcert.pem -nam
e "manuel" -out priv-pkcs12_MC.p12
Enter Export Password:
Verifying - Enter Export Password:
manuel@manuel-X550CL:~/MEGAsync/Universidade/SRC/TP2/MC/12$
```

Figura 12 - Comandos para criar ficheiro PKCS#12.

13- Instalação de todos os certificados no Sistema Operativo

13.1- Windows

Duplo clique em cima do certificado e abre o gestor de certificados do Windows como se pode ver na Figura 13.

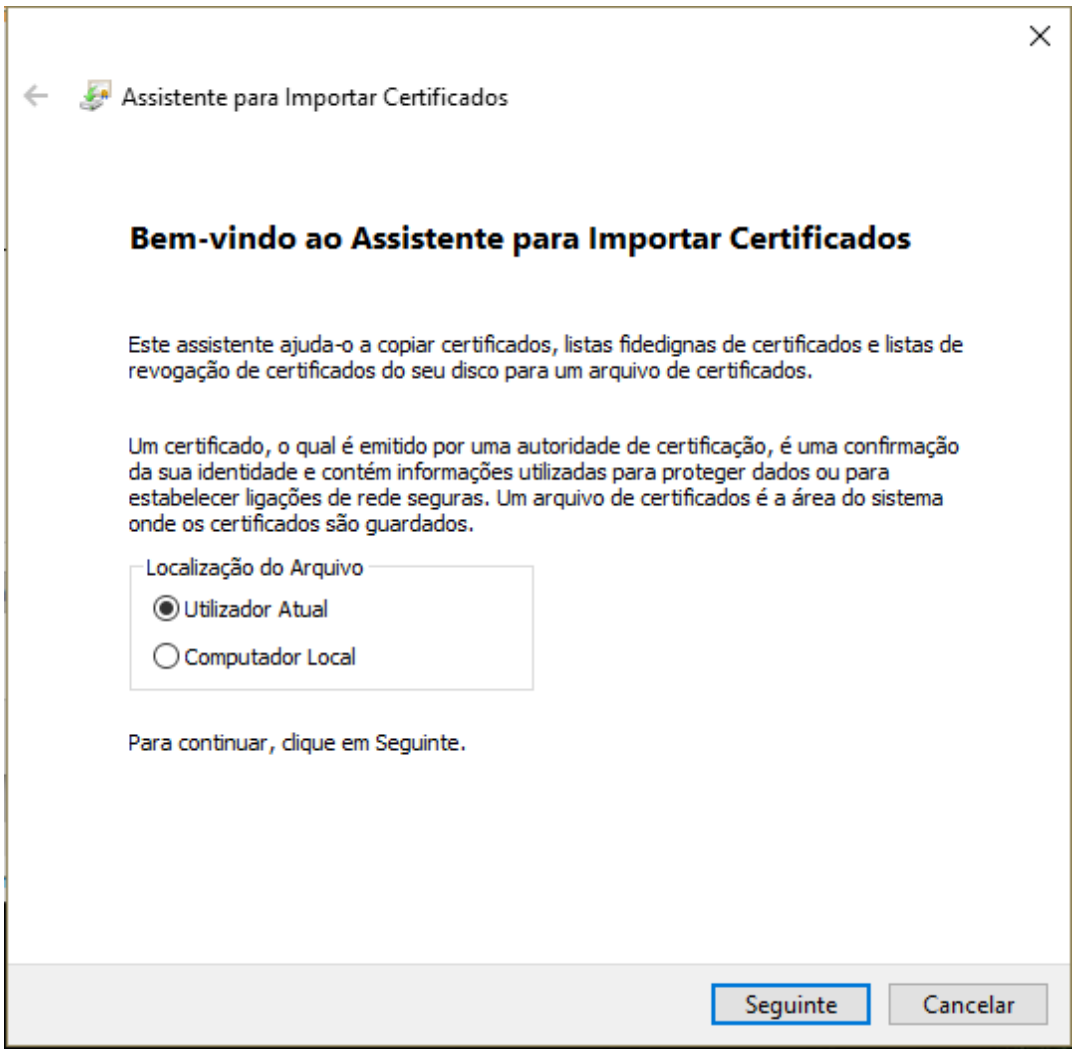


Figura 13 - Gestor de certificados do Windows.

Vão aparecer alguns menus dos quais apenas é relevante mostrar o da Figura 14 que representa o menu onde pede pela password do certificado:

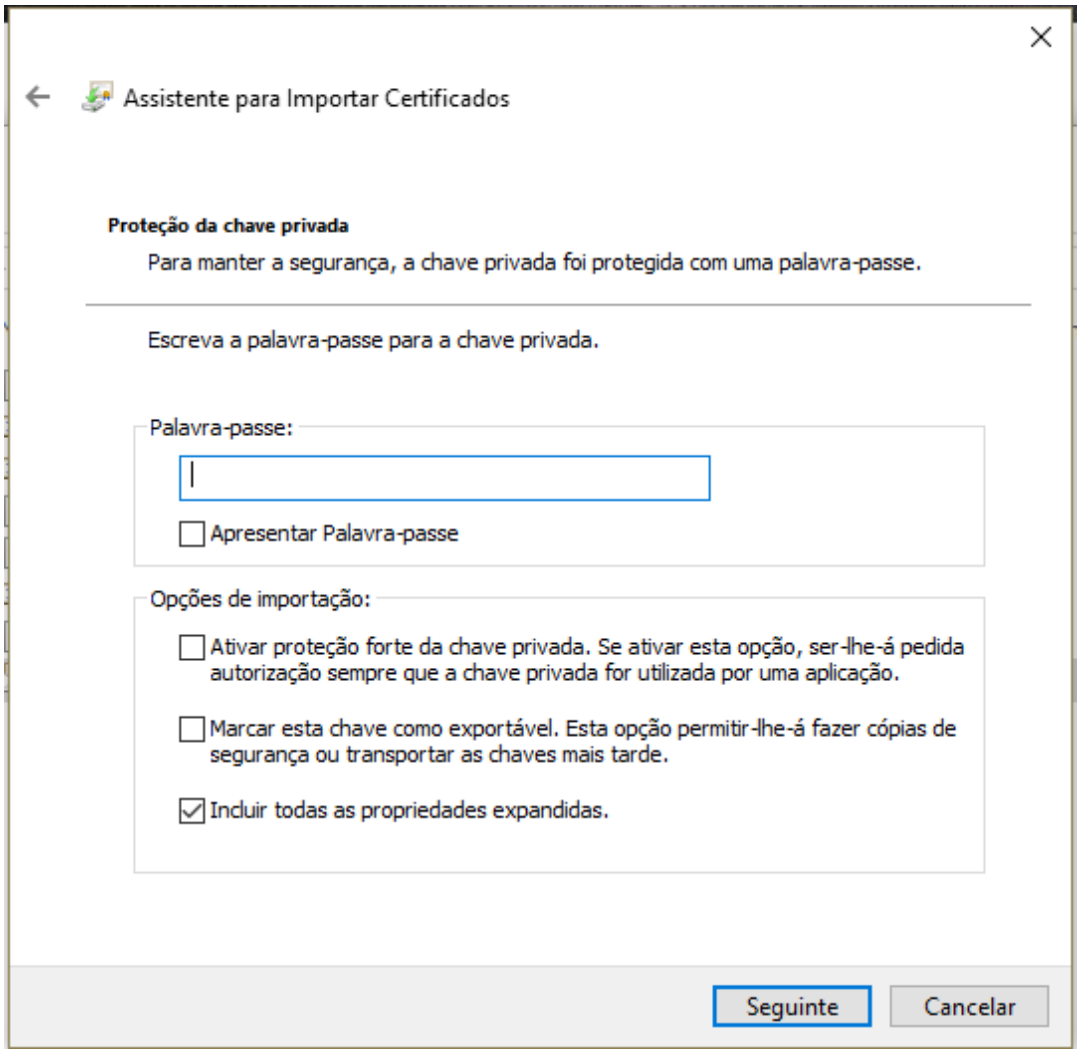


Figura 14 - Pedido de password para importar o certificado.

No caso dos certificados pessoais a única diferença será no passo da password, que para este caso não vai existir pois, sendo um certificado público, é de utilização livre.

Parte 2 - Enviar e receber mensagens seguras

1- Inserir o certificado P12 no *Outlook*

Para inserir o certificado no Outlook 2016 é necessário aceder ás definições da "Central de Confiabilidade", seguido da opção na lateral esquerda de "Segurança de Email" selecionar no menu da direita, na secção de "Identificações Digitais (Certificados)", e selecionar "Importar". Deverá aparecer um menu similar ao da Figura 15:

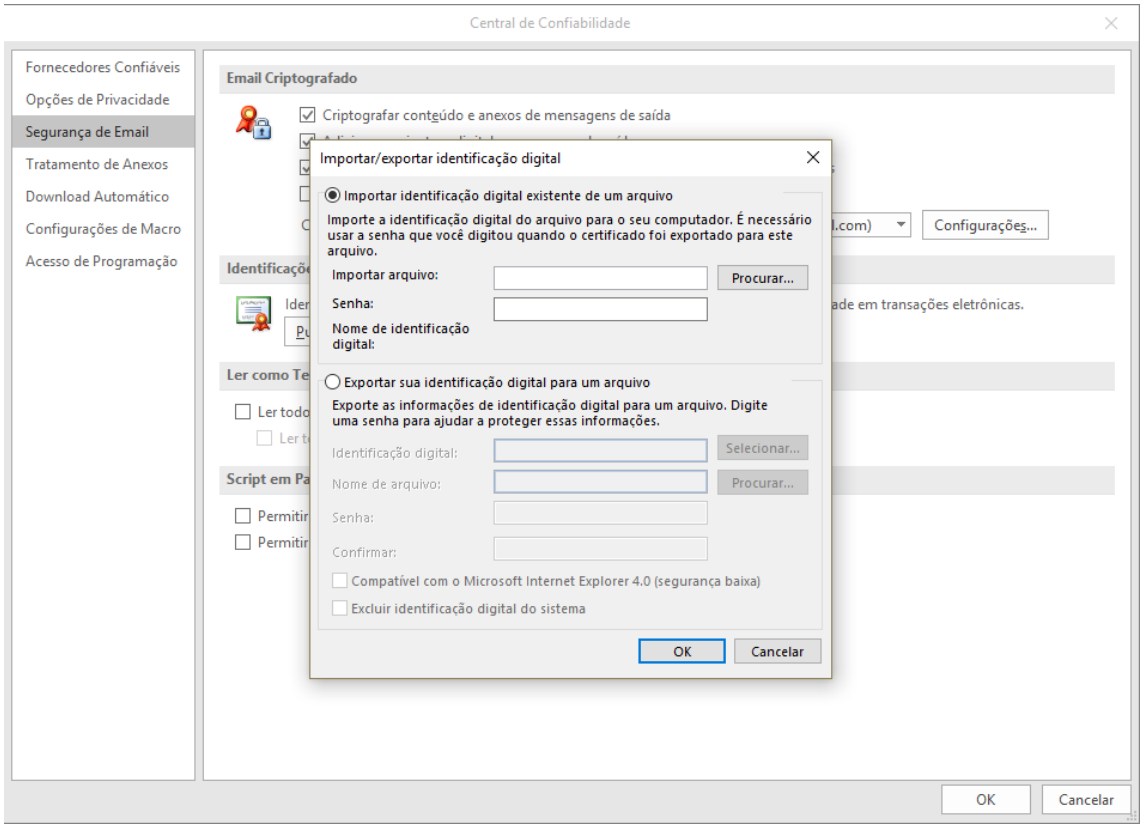


Figura 15 - Importação da chave privada (p12).

Neste menu deverá selecionar a chave privada e colocar a *passphrase* correspondente.

Após importar o certificado é necessário seleciona-lo na secção "Email Criptografado" e seleciona-lo como *default*.

2- Importação dos certificados pessoais para o Outlook 2016

Para se poder encriptar um email é necessário importar os certificados de cada um dos destinatários de forma a cifrar a mensagem com a sua chave publica. Para que isto seja possível é necessário criar novo contacto e adicionar o seu certificado, como se pode ver na Figura 16.

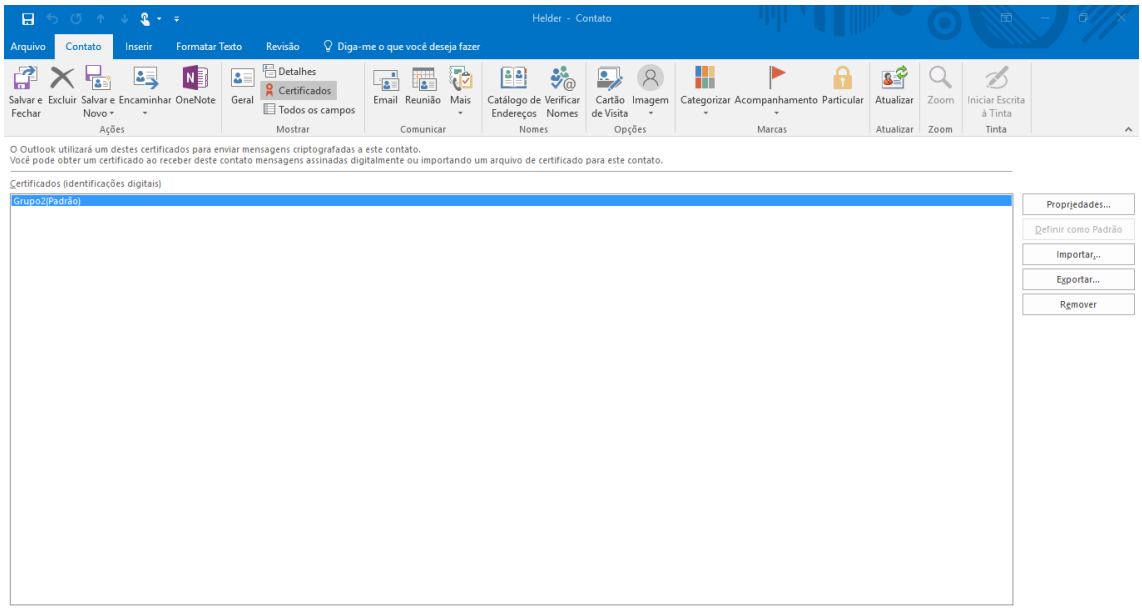


Figura 16 - Importar certificado pessoal do contato.

É necessário repetir este processo para cada um dos destinatários que se pretende usar encriptação de email.

A partir deste momento sempre que se abre o Outlook e sempre que se acede a um email que esteja encriptado é necessário introduzir a nossa "*passphrase*". Na **Error!**

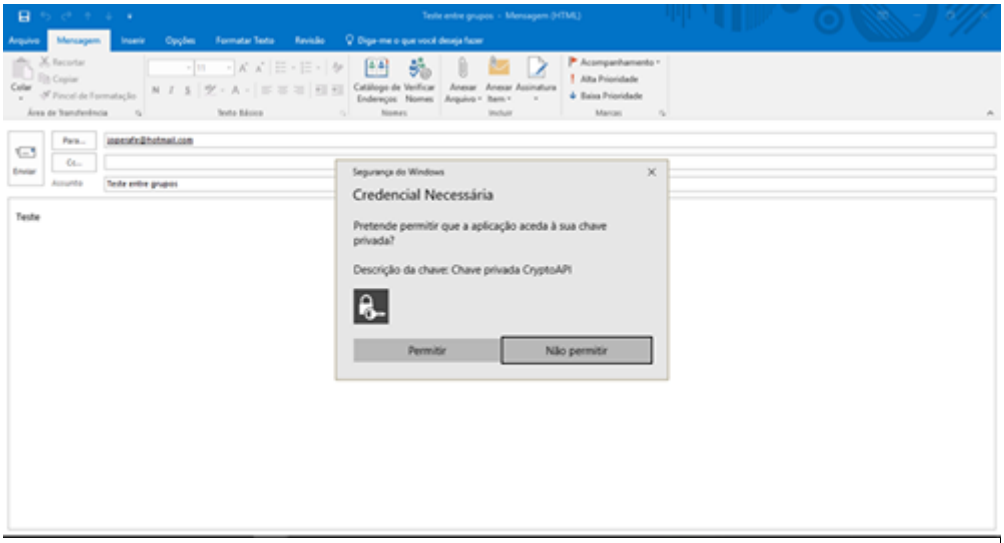


Figura 17 - Pedido da password para aceder à chave privada para assinar um e-mail.

Reference source not found. , encontra-se um pedido de *password para* assinar e encriptar um e-mail.

3- Troca de emails encriptados e assinados

3.1- Entre elementos do mesmo grupo

Receção na Figura 19 e envio na Figura 18.

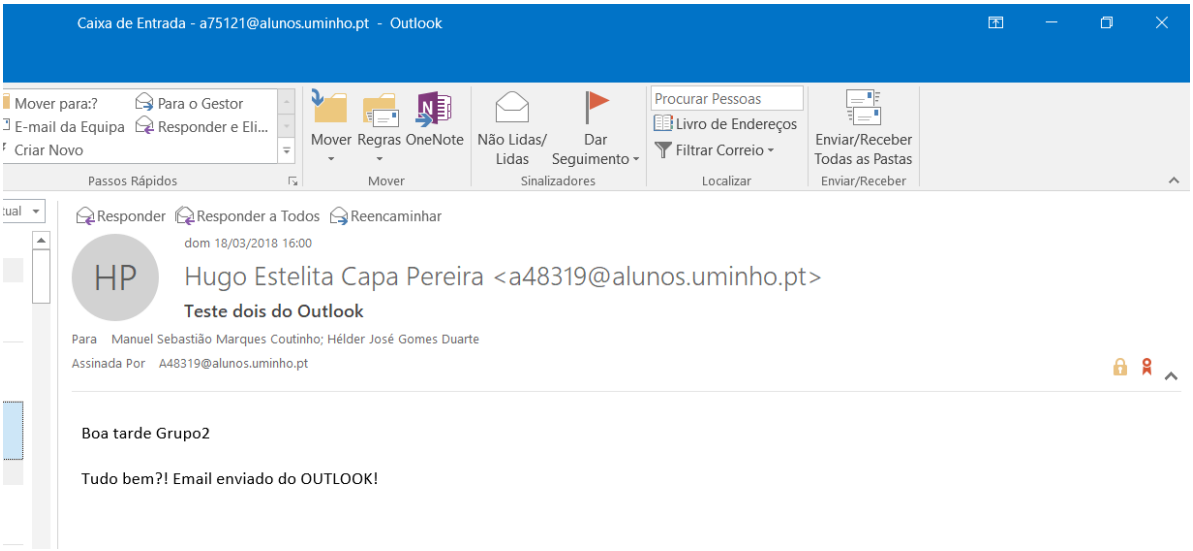


Figura 19 – Email recebido desencriptado e digitalmente assinado por um elemento do grupo.

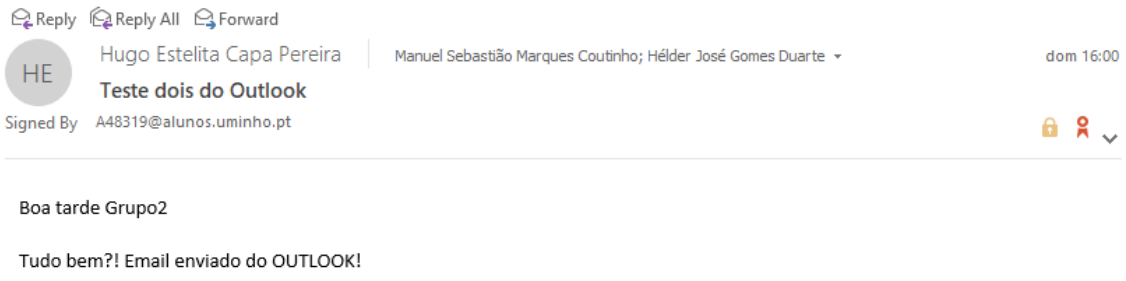


Figura 18 - Email enviado encriptado e assinado por um elemento do grupo.

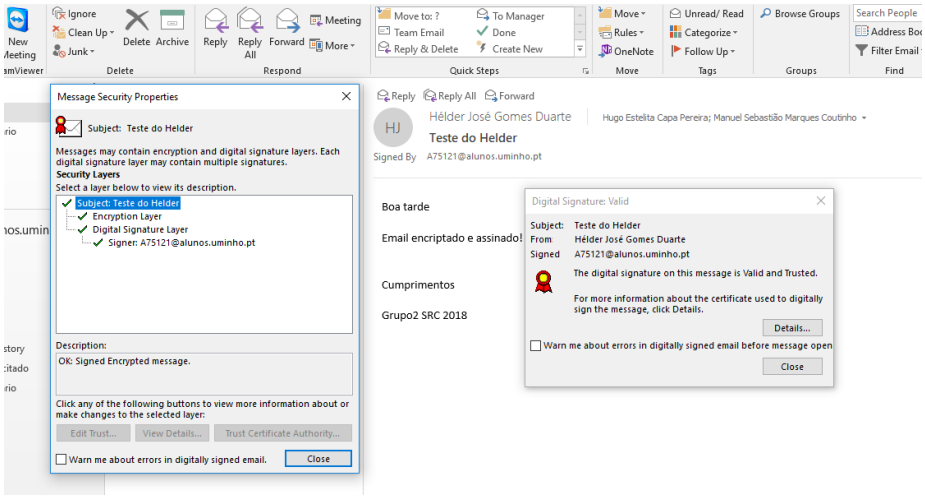


Figura 20 – Visualização do certificado e respetiva assinatura digital.

3.2- Entre os nossos elementos e os elementos do grupo 3.

A Figura 21 representa o email enviado por nos e a Figura 22 o email recebido por nós.

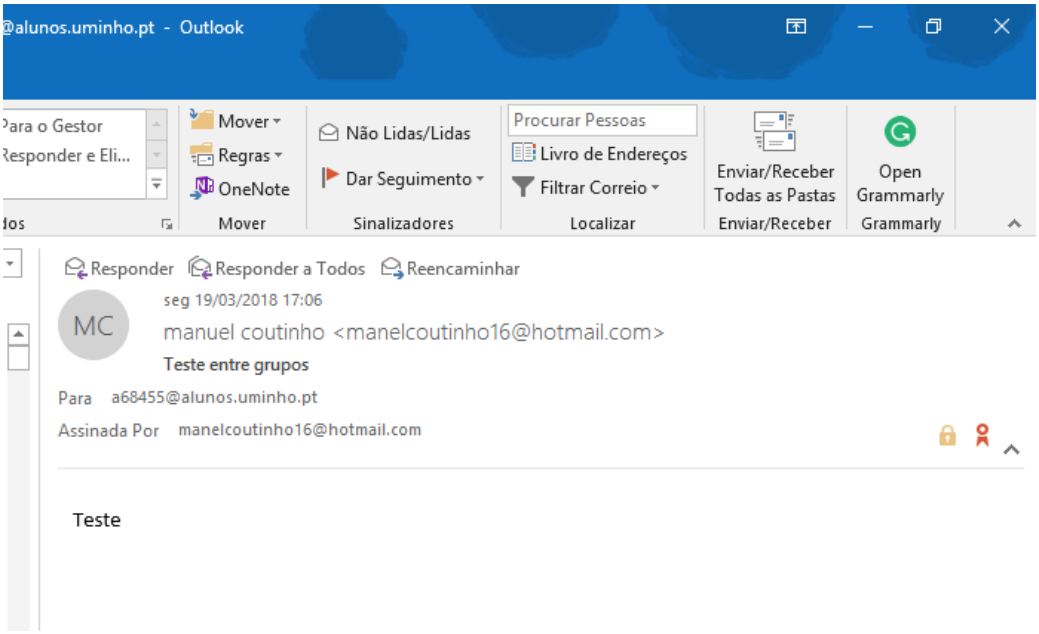


Figura 21 - Email enviado do nosso grupo para um elemento do grupo 3.

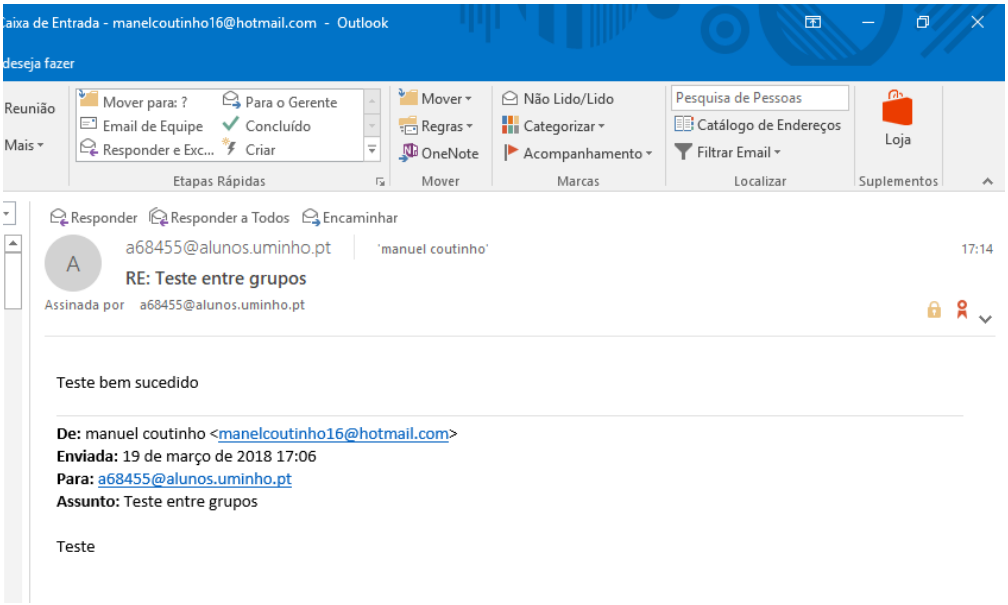


Figura 22 - Email do grupo 2, recebido pelo grupo 3.

4- Revogação de um certificado.

Para efetuar a revogação de um certificado foi necessário ir ao servidor e executar a instrução "*Revoke*" como pode ser visto na Figura 23.

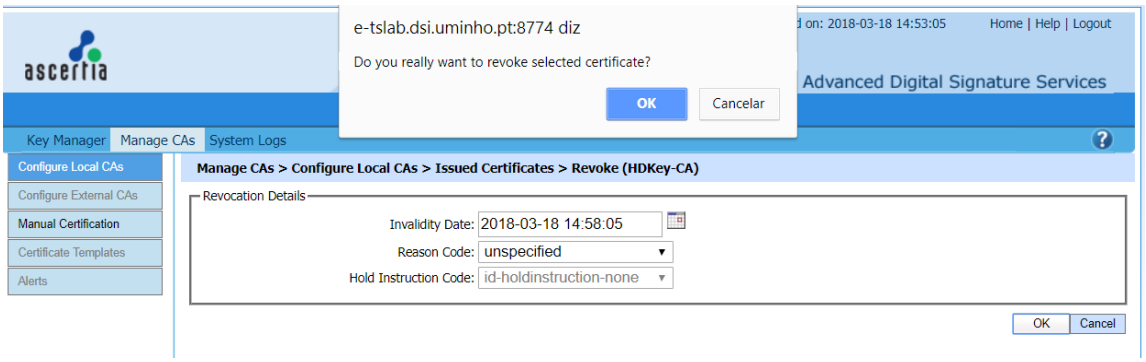


Figura 23-Revogação de um certificado.

Na Figura 24**Error! Reference source not found.** é visível a confirmação da

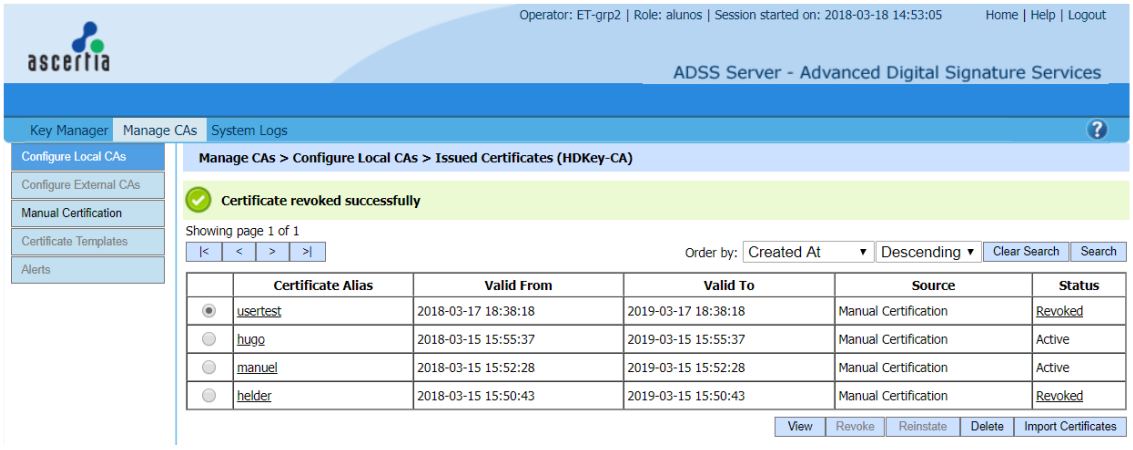


Figura 24 - Certificados após revogação.

revogação do certificado.

Na Figura **Error! Reference source not found.** podemos ver o passo necessário à importação da CRL para o nosso computador.

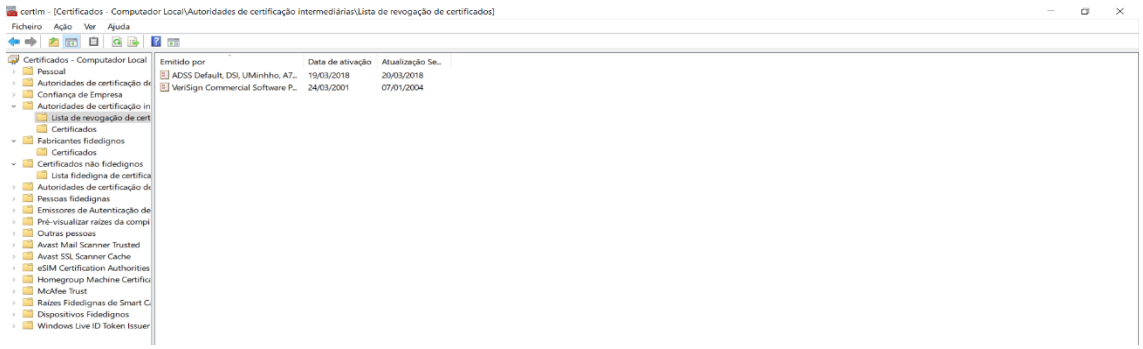


Figura 25 - Importação da nossa CRL para o nosso computador.

Na Figura é visível que o certificado foi revogado tendo em conta que já se encontra adicionado à CRL.

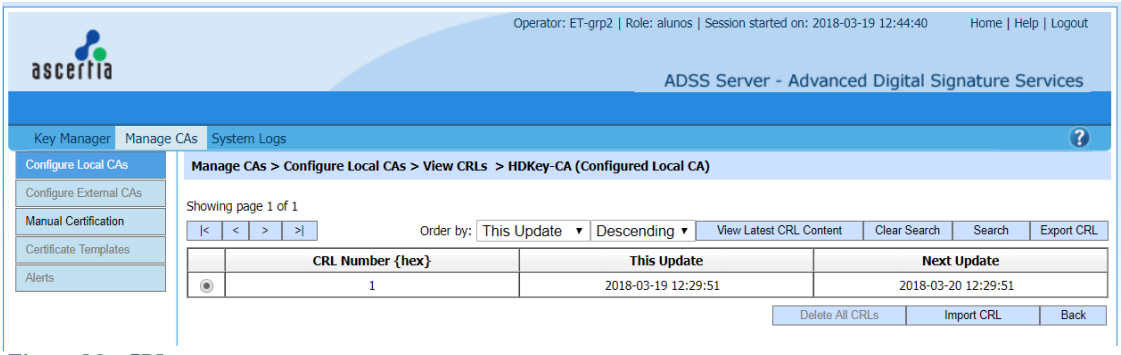


Figura 26 - CRLs.

Na Figura é possível ver que após a revogação do certificado, não é possível encriptar a mensagem visto não dispor do certificado.

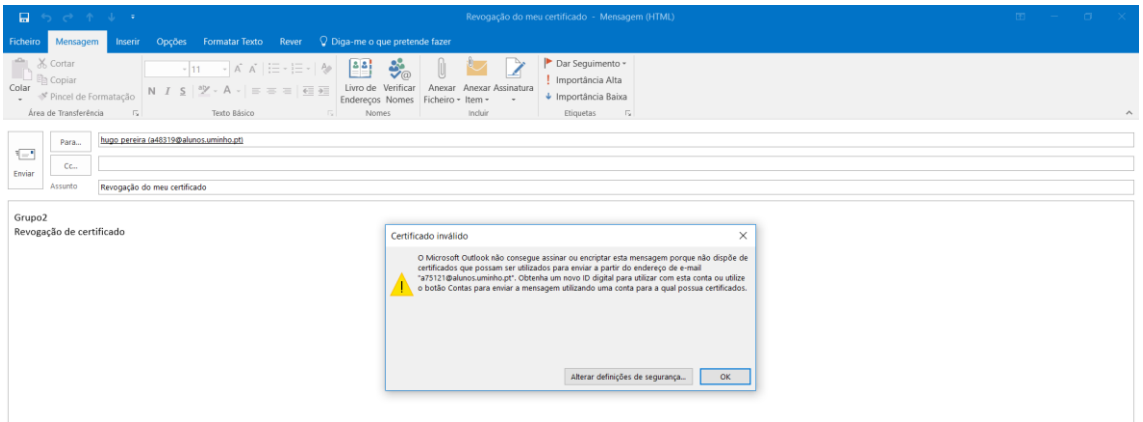


Figura 27 - Incapacidade para encriptar mensagem devido à falta de certificado.

5- Resposta à pergunta sobre outras possibilidades sobre a criação de relações de confiança entre diversas CAs.

Apesar de termos sido conduzidos para a criação de uma CA de raiz, não é estritamente necessário que a sua criação seja feita dessa forma visto que o paradigma de "Web of Trust" não o faz. Em vez disso os utilizadores confiam nos certificados dos outros tal como nós fizemos. Isto também podia ter sido feito através de PGP.

6- Conclusão

Após a realização deste trabalho prático aprendemos como funcionam as cadeias de certificação, a sua hierarquia, e a relação de confiança estabelecida entre as diversas autoridades de certificação. Aprendemos também a implementar na prática um sistema seguro para encriptar e assinar dados para os podermos trocar com outras pessoas sem estarmos expostos às diversas vulnerabilidades existentes.