Aluno: Quenio Cesar Machado dos Santos
Matricula: 14100868
Disciplina: INE5429 - Segurança em Computadores
Data: 04/12/2016

Relatório: Confiança em certificados Digitais PGP

a) Assinar os certificados de todos os seus colegas e do professor.

Para assinar o certificado que os colegas criaram na aula anterior, é preciso primeiro baixá-los do servidor de chaves da RNP usando o comando abaixo:

```
$ gpg --keyserver raxus.rnp.br --recv-key cfafe5bd
gpg: requesting key CFAFE5BD from hkp server raxus.rnp.br
gpg: key CFAFE5BD: public key "Guilherme Nakayama (INE5429) <guilherme.nakayama@hotmail.com>" imported
gpg: 3 marginal(s) needed, 1 complete(s) needed, PGP trust model
gpg: depth: 0  valid:   1  signed:   2  trust: 0-, 0q, 0n, 0m, 0f, 1u
gpg: depth: 1  valid:   2  signed:   0  trust: 1-, 0q, 0n, 0m, 1f, 0u
gpg: next trustdb check due at 2016-08-03
gpg: Total number processed: 1
gpg:               imported: 1  (RSA: 1)
```

Agora, para assinar o certificado do colega, utiliza-se o comando para editar o certificado, verificar sua "fingerprint" e assiná-lo:

```
$ gpg --edit-key guilherme.nakayama@hotmail.com
gpg (GnuPG) 1.4.20; Copyright (C) 2015 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.


pub  2048R/CFAFE5BD  created: 2016-04-05  expires: 2016-07-04  usage: SC
                     trust: unknown       validity: unknown
sub  2048R/0BAD2D62  created: 2016-04-05  expires: 2016-07-04  usage: E
[ unknown] (1). Guilherme Nakayama (INE5429) <guilherme.nakayama@hotmail.com>
[ unknown] (2)  Guilherme Nakayama <guilherme.nakayama@hotmail.com>

gpg> fpr
pub   2048R/CFAFE5BD 2016-04-05 Guilherme Nakayama (INE5429) <guilherme.nakayama@hotmail.com>
 Primary key fingerprint: D55C 0679 DA26 5D96 3B9D  F5DC DE27 BE97 CFAF E5BD

gpg> sign
Really sign all user IDs? (y/N) y

pub  2048R/CFAFE5BD  created: 2016-04-05  expires: 2016-07-04  usage: SC
                     trust: unknown       validity: unknown
 Primary key fingerprint: D55C 0679 DA26 5D96 3B9D  F5DC DE27 BE97 CFAF E5BD

     Guilherme Nakayama (INE5429) <guilherme.nakayama@hotmail.com>
     Guilherme Nakayama <guilherme.nakayama@hotmail.com>

This key is due to expire on 2016-07-04.
Are you sure that you want to sign this key with your
key "Quenio Cesar Machado dos Santos (Ver...) <queniodossantos@gmail.com>" (B03C59BB)

Really sign? (y/N) y

You need a passphrase to unlock the secret key for
user: "Quenio Cesar Machado dos Santos (Ver...) <queniodossantos@gmail.com>"
2048-bit RSA key, ID B03C59BB, created 2016-04-05


gpg> quit
Save changes? (y/N) y
```

b) Verificar como se deve proceder para a atualização dos certificados (conhecidos como anéis de chaves PGP) privados e públicos.

Uma vez assinado o certificado do colega, é preciso enviá-lo para o servidor de chaves da RNP para que seja incluída nossa assinatura:

```
$ gpg --keyserver raxus.rnp.br --send-key CFAFE5BD
gpg: sending key CFAFE5BD to hkp server raxus.rnp.br
```

Verificando o servidor da RNP, minha assinatura agora se encontra no certificado do colega:

```
pub  2048R/CFAFE5BD 2016-04-05            uid Guilherme Nakayama <guilherme.nakayama@hotmail.com>
sig  sig3  CFAFE5BD 2016-04-05 __________ 2016-07-04 [selfsig]
sig  sig   E62976D7 2016-04-12 __________ __________ Ranieri Althoff (Key for INE5429) <ranisalt@gmail.com>
sig  sig   7681F1FB 2016-04-12 __________ __________ Ion JosÃ© de Souza Neto <ionneto@gmail.com>
sig  sig   2F3EE36E 2016-04-12 __________ __________ Lucas Finger Roman <lfrfinger@gmail.com>
sig  sig   0DC62EBB 2016-04-12 __________ __________ Willian de Souza <willianstosouza@gmail.com>
sig  sig   B03C59BB 2016-04-12 __________ __________ Quenio Cesar Machado dos Santos (Ver...) <queniodossantos@gmail.com>uid Guilherme Nakayama (IN
sig  sig3  CFAFE5BD 2016-04-12 __________ 2016-07-04 [selfsig]
sig  sig   0DC62EBB 2016-04-12 __________ __________ Willian de Souza <willianstosouza@gmail.com>
sig  sig   B03C59BB 2016-04-12 __________ __________ Quenio Cesar Machado dos Santos (Ver...) <queniodossantos@gmail.com>sub  2048R/0BAD2D62 2016-0
sig sbind  CFAFE5BD 2016-04-05 __________ 2016-07-04 []
```

c) Criar um certificado PGP, incluir tal certificado num servidor remoto e depois revogá-lo.

Abaixo, criamos um novo certificado PGP:

```
$ gpg --gen-key
gpg (GnuPG) 1.4.20; Copyright (C) 2015 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Please select what kind of key you want:
   (1) RSA and RSA (default)
   (2) DSA and Elgamal
   (3) DSA (sign only)
   (4) RSA (sign only)
Your selection? 1
RSA keys may be between 1024 and 4096 bits long.
What keysize do you want? (2048)
Requested keysize is 2048 bits
Please specify how long the key should be valid.
         0 = key does not expire
      <n>  = key expires in n days
      <n>w = key expires in n weeks
      <n>m = key expires in n months
      <n>y = key expires in n years
Key is valid for? (0) 2
Key expires at Fri Apr 15 16:16:16 2016 BRT
Is this correct? (y/N) y

You need a user ID to identify your key; the software constructs the user ID
from the Real Name, Comment and Email Address in this form:
    "Heinrich Heine (Der Dichter) <heinrichh@duesseldorf.de>"

Real name: Q S
Name must be at least 5 characters long
Real name: Quenio Santos
Email address: quenio@me.com
Comment: Temp Key
You selected this USER-ID:
    "Quenio Santos (Temp Key) <quenio@me.com>"

Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit? O
You need a Passphrase to protect your secret key.

We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
......+++++
...+++++
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
....+++++
..+++++
gpg: key FE6C38CE marked as ultimately trusted
public and secret key created and signed.

gpg: checking the trustdb
gpg: 3 marginal(s) needed, 1 complete(s) needed, PGP trust model
gpg: depth: 0  valid:   2  signed:   3  trust: 0-, 0q, 0n, 0m, 0f, 2u
gpg: depth: 1  valid:   3  signed:   0  trust: 2-, 0q, 0n, 0m, 1f, 0u
gpg: next trustdb check due at 2016-04-15
pub   2048R/FE6C38CE 2016-04-13 [expires: 2016-04-15]
      Key fingerprint = 5375 AA33 8DA3 40B7 D6F0  DF72 03B1 8C70 FE6C 38CE
uid                  Quenio Santos (Temp Key) <quenio@me.com>
sub   2048R/6E7FB5EC 2016-04-13 [expires: 2016-04-15]
```

Enviando o novo certificado para o servidor da RNP:

```
gpg --keyserver raxus.rnp.br --send-key FE6C38CE
gpg: sending key FE6C38CE to hkp server raxus.rnp.br
```

Agora, o certificado se encontra no servidor RNP:

```
pub  2048R/FE6C38CE 2016-04-13            uid Quenio Santos (Temp Key) <quenio@me.com>
sig  sig3  FE6C38CE 2016-04-13 __________ 2016-04-15 [selfsig]sub  2048R/6E7FB5EC 2016-04-13
sig sbind  FE6C38CE 2016-04-13 __________ 2016-04-15 []
```

Gerando o certificado de revogação:

```
gpg --output qs.revoke.asc  --gen-revoke FE6C38CE

sec  2048R/FE6C38CE 2016-04-13 Quenio Santos (Temp Key) <quenio@me.com>

Create a revocation certificate for this key? (y/N) y
Please select the reason for the revocation:
  0 = No reason specified
  1 = Key has been compromised
  2 = Key is superseded
  3 = Key is no longer used
  Q = Cancel
(Probably you want to select 1 here)
Your decision? 0
Enter an optional description; end it with an empty line:
> Temp key for school exercise.
>
Reason for revocation: No reason specified
Temp key for school exercise.
Is this okay? (y/N) y

You need a passphrase to unlock the secret key for
user: "Quenio Santos (Temp Key) <quenio@me.com>"
2048-bit RSA key, ID FE6C38CE, created 2016-04-13

ASCII armored output forced.
Revocation certificate created.

Please move it to a medium which you can hide away; if Mallory gets
access to this certificate he can use it to make your key unusable.
It is smart to print this certificate and store it away, just in case
your media become unreadable.  But have some caution:  The print system of
your machine might store the data and make it available to others!
```

Agora, importamos o certificado de revogação no GnuPG:

```
$ gpg --import qs.revoke.asc
gpg: key FE6C38CE: "Quenio Santos (Temp Key) <quenio@me.com>" revocation certificate imported
gpg: Total number processed: 1
gpg:    new key revocations: 1
gpg: 3 marginal(s) needed, 1 complete(s) needed, PGP trust model
gpg: depth: 0  valid:   2  signed:   3  trust: 0-, 0q, 0n, 0m, 0f, 2u
gpg: depth: 1  valid:   3  signed:   0  trust: 2-, 0q, 0n, 0m, 1f, 0u
gpg: next trustdb check due at 2016-04-15
```

Finalmente, enviamos a revogação para o servidor RNP:

```
gpg --keyserver raxus.rnp.br --send-key FE6C38CE
gpg: sending key FE6C38CE to hkp server raxus.rnp.br
```

Agora, o servidor RNP já confirmou a revogação:

```
pub  2048R/FE6C38CE 2016-04-13
sig revok  FE6C38CE 2016-04-13 __________ __________ [selfsig]uid Quenio Santos (Temp Key) <quenio@me.com>
sig  sig3  FE6C38CE 2016-04-13 __________ 2016-04-15 [selfsig]sub  2048R/6E7FB5EC 2016-04-13
sig sbind  FE6C38CE 2016-04-13 __________ 2016-04-15 []
```

d) É possível ter mais de uma chave em um mesmo certificado PGP? Se sim, gere tal certificado.

Sim. É possível adicionar mais chaves a um mesmo certificado PGP, como ilustrado abaixo:

```
$ gpg --edit-key queniodossantos@gmail.com
gpg (GnuPG) 1.4.20; Copyright (C) 2015 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Secret key is available.

pub  2048R/B03C59BB  created: 2016-04-05  expires: 2016-08-03  usage: SC
                     trust: ultimate      validity: ultimate
sub  2048R/5395414D  created: 2016-04-05  expires: 2016-08-03  usage: E
[ultimate] (1). Quenio Cesar Machado dos Santos (Ver...) <queniodossantos@gmail.com>

gpg> addkey
Key is protected.

You need a passphrase to unlock the secret key for
user: "Quenio Cesar Machado dos Santos (Ver...) <queniodossantos@gmail.com>"
2048-bit RSA key, ID B03C59BB, created 2016-04-05

Please select what kind of key you want:
   (3) DSA (sign only)
   (4) RSA (sign only)
   (5) Elgamal (encrypt only)
   (6) RSA (encrypt only)
Your selection? 5
ELG-E keys may be between 1024 and 4096 bits long.
What keysize do you want? (2048)
Requested keysize is 2048 bits
Please specify how long the key should be valid.
         0 = key does not expire
      <n>  = key expires in n days
      <n>w = key expires in n weeks
      <n>m = key expires in n months
      <n>y = key expires in n years
Key is valid for? (0) 120
Key expires at Thu Aug 11 22:16:34 2016 BRT
Is this correct? (y/N) y
```

```
Really create? (y/N) y
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
.+++++++++++++++++++++++++.+++++...+++++++++++++++++++++++++++++++++.++++++++++.++++++++++++++++++++++++++++++++++.+++++.++++++++++++++.+++++++

pub  2048R/B03C59BB  created: 2016-04-05  expires: 2016-08-03  usage: SC
                     trust: ultimate      validity: ultimate
sub  2048R/5395414D  created: 2016-04-05  expires: 2016-08-03  usage: E
sub  2048g/91AC5577  created: 2016-04-14  expires: 2016-08-12  usage: E
[ultimate] (1). Quenio Cesar Machado dos Santos (Ver...) <queniodossantos@gmail.com>

gpg> list

pub  2048R/B03C59BB  created: 2016-04-05  expires: 2016-08-03  usage: SC
                     trust: ultimate      validity: ultimate
sub  2048R/5395414D  created: 2016-04-05  expires: 2016-08-03  usage: E
sub  2048g/91AC5577  created: 2016-04-14  expires: 2016-08-12  usage: E
[ultimate] (1). Quenio Cesar Machado dos Santos (Ver...) <queniodossantos@gmail.com>
```

e) O que são sub-chaves? Para que servem? Mostre um exemplo.

As sub-chaves, como àquela adicionada no item acima, permitem que se atualize as chaves periodicamente sem a necessidade de criar um novo certificado, o que exigiria recriar a cadeia de confiança.

Assim, caso uma sub-chave seja comprometida, é possível criar uma nova sub-chave com o mesmo certificado para substituir a chave comprometida.

Abaixo, tem-se o exemplo da sub-chave criada no item anterior já regitrada com o servidor da RNP:

```
pub  2048R/B03C59BB 2016-04-05            uid Quenio Cesar Machado dos Santos (Ver...) <queniodossantos@gmail.com>
sig  sig3  B03C59BB 2016-04-05 __________ 2016-08-03 [selfsig]
sig  sig   2B55081E 2016-04-12 __________ __________ Giovanni Antonio Tomaso Ferreira Rotta (Chave) <giovanni_rotta@hotmail.com>
sig  sig   B0721698 2016-04-13 __________ __________ Gustavo Jose Carpeggiani (NOVA) <g.j.carpeggiani@grad.ufsc.br>
sig  sig   D3032F08 2016-04-13 __________ __________ Cesar 2 (segunda identidade) <cesar.junior@grad.ufsc.br>
sig  sig   873532D4 2016-04-13 __________ __________ Diego Almeida de Oliveira <diegohkd@hotmail.com>
sig  sig   0DC62EBB 2016-04-13 __________ __________ Willian de Souza <willianstosouza@gmail.com>
sig  sig   5D24C4C3 2016-04-13 __________ __________ Igor d. S. S. (.-. nova .-.) <gursol@yahoo.com.br>
sig  sig   2B004CD1 2016-04-14 __________ __________ Abraham Jean (New Key) <abramuus@hotmail.com>sub  2048R/5395414D 2016-04-05
sig sbind  B03C59BB 2016-04-05 __________ 2016-08-03 []sub  2048g/91AC5577 2016-04-14
sig sbind  B03C59BB 2016-04-14 __________ 2016-08-12 []
```

f) Que tipo de atributos um certificado PGP pode conter? Seria possível adicionar sua foto no certificado? Que garantias há de que tal foto não pode ser modificada por agentes maliciosos?

Sim. É possível adicionar uma foto à chave como demonstrado abaixo:

```
$ gpg --edit-key queniodossantos@gmail.com
gpg (GnuPG) 1.4.20; Copyright (C) 2015 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Secret key is available.

pub  2048R/B03C59BB  created: 2016-04-05  expires: 2016-08-03  usage: SC
                     trust: ultimate      validity: ultimate
sub  2048R/5395414D  created: 2016-04-05  expires: 2016-08-03  usage: E
sub  2048g/91AC5577  created: 2016-04-14  expires: 2016-08-12  usage: E
[ultimate] (1). Quenio Cesar Machado dos Santos (Ver...) <queniodossantos@gmail.com>

gpg> addphoto

Pick an image to use for your photo ID.  The image must be a JPEG file.
Remember that the image is stored within your public key.  If you use a
very large picture, your key will become very large as well!
Keeping the image close to 240x288 is a good size to use.

Enter JPEG filename for photo ID: /Users/Quenio/Pictures/profile-small.jpg
This JPEG is really large (20690 bytes) !
Are you sure you want to use it? (y/N) y
Is this photo correct (y/N/q)? y

You need a passphrase to unlock the secret key for
user: "Quenio Cesar Machado dos Santos (Ver...) <queniodossantos@gmail.com>"
2048-bit RSA key, ID B03C59BB, created 2016-04-05


pub  2048R/B03C59BB  created: 2016-04-05  expires: 2016-08-03  usage: SC
                     trust: ultimate      validity: ultimate
sub  2048R/5395414D  created: 2016-04-05  expires: 2016-08-03  usage: E
sub  2048g/91AC5577  created: 2016-04-14  expires: 2016-08-12  usage: E
[ultimate] (1). Quenio Cesar Machado dos Santos (Ver...) <queniodossantos@gmail.com>
[ unknown] (2)  [jpeg image of size 20690]

Save changes? (y/N) y
```

Uma vez adicionada ao certificado, a foto não pode ser alterada, pois ela foi assinada com a chave master, da mesma forma que todas as outras informações contidas no certificado.

Além da photo, também é possivel adicionar mais user ids, com novos nomes e emails.

g) É possível mudar ou adcionar atributos depois que o certificado já tiver sido publicado nos servidores PGP?

Sim. É possível adicionar novos user ids, com novos nomes e emails, e depois distribuí-los para o servidor de chave, como feito abaixo para o servidor RNP:

```
$ gpg --edit-key queniodossantos@gmail.com
gpg (GnuPG) 1.4.20; Copyright (C) 2015 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Secret key is available.

pub  2048R/B03C59BB  created: 2016-04-05  expires: 2016-08-03  usage: SC
                     trust: ultimate      validity: ultimate
sub  2048R/5395414D  created: 2016-04-05  expires: 2016-08-03  usage: E
sub  2048g/91AC5577  created: 2016-04-14  expires: 2016-08-12  usage: E
[ultimate] (1). Quenio Cesar Machado dos Santos (Ver...) <queniodossantos@gmail.com>
[ultimate] (2)  [jpeg image of size 20690]

gpg> adduid
Real name: Quenio C M dos Santos
Email address: quenio@me.com
Comment: Email Alternativo
You selected this USER-ID:
    "Quenio C M dos Santos (Email Alternativo) <quenio@me.com>"

Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit? O

You need a passphrase to unlock the secret key for
user: "Quenio Cesar Machado dos Santos (Ver...) <queniodossantos@gmail.com>"
2048-bit RSA key, ID B03C59BB, created 2016-04-05


pub  2048R/B03C59BB  created: 2016-04-05  expires: 2016-08-03  usage: SC
                     trust: ultimate      validity: ultimate
sub  2048R/5395414D  created: 2016-04-05  expires: 2016-08-03  usage: E
sub  2048g/91AC5577  created: 2016-04-14  expires: 2016-08-12  usage: E
[ultimate] (1)  Quenio Cesar Machado dos Santos (Ver...) <queniodossantos@gmail.com>
[ultimate] (2)  [jpeg image of size 20690]
[ unknown] (3). Quenio C M dos Santos (Email Alternativo) <quenio@me.com>

Save changes? (y/N) y

$ gpg --keyserver raxus.rnp.br --send-key B03C59BB
gpg: sending key B03C59BB to hkp server raxus.rnp.br

pub  2048R/B03C59BB 2016-04-05            uid Quenio C M dos Santos (Email Alternativo) <quenio@me.com>
sig  sig3  B03C59BB 2016-04-14 __________ 2016-08-03 [selfsig]uid Quenio Cesar Machado dos Santos (Ver...) <queniodossantos@gmail.com>
sig  sig3  B03C59BB 2016-04-05 __________ 2016-08-03 [selfsig]
sig  sig   2B55081E 2016-04-12 __________ __________ Giovanni Antonio Tomaso Ferreira Rotta (Chave) <giovanni_rotta@hotmail.com>
sig  sig   B0721698 2016-04-13 __________ __________ Gustavo Jose Carpeggiani (NOVA) <g.j.carpeggiani@grad.ufsc.br>
sig  sig   D3032F08 2016-04-13 __________ __________ Cesar 2 (segunda identidade) <cesar.junior@grad.ufsc.br>
sig  sig   873532D4 2016-04-13 __________ __________ Diego Almeida de Oliveira <diegohkd@hotmail.com>
sig  sig   0DC62EBB 2016-04-13 __________ __________ Willian de Souza <willianstosouza@gmail.com>
sig  sig   5D24C4C3 2016-04-13 __________ __________ Igor d. S. S. (.-. nova .-.) <gursol@yahoo.com.br>
sig  sig   2B004CD1 2016-04-14 __________ __________ Abraham Jean (New Key) <abramuus@hotmail.com>uat [contents omitted]
sig  sig3  B03C59BB 2016-04-14 __________ 2016-08-03 [selfsig]sub  2048R/5395414D 2016-04-05
sig sbind  B03C59BB 2016-04-05 __________ 2016-08-03 []sub  2048g/91AC5577 2016-04-14
sig sbind  B03C59BB 2016-04-14 __________ 2016-08-12 []
```

h) É possível revogar a sua assinatura de um certificado PGP de outrem (que você anteriormente assinou)? Se sim, mostre um exemplo.

Sim, é possível revogar minha assinatura de um outro certificado PGP, como ilustrado abaixo:

```
$ gpg --edit-key custodio@inf.ufsc.br
gpg (GnuPG) 1.4.20; Copyright (C) 2015 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.


pub  1024D/DC26872D  created: 2002-03-16  expires: never       usage: SC
                     trust: full          validity: full
sub  2048g/4C24E598  created: 2002-03-16  expires: never       usage: E
[  full  ] (1). Ricardo Felipe Cust\xf3\x64io <custodio@inf.ufsc.br>

gpg> revsig
You have signed these user IDs on key DC26872D:
     Ricardo Felipe Cust\xf3\x64io <custodio@inf.ufsc.br>
   signed by your key B03C59BB on 2016-04-12

user ID: "Ricardo Felipe Cust\xf3\x64io <custodio@inf.ufsc.br>"
signed by your key B03C59BB on 2016-04-12
Create a revocation certificate for this signature? (y/N) y
You are about to revoke these signatures:
     Ricardo Felipe Cust\xf3\x64io <custodio@inf.ufsc.br>
   signed by your key B03C59BB on 2016-04-12
Really create the revocation certificates? (y/N) y
Please select the reason for the revocation:
  0 = No reason specified
  4 = User ID is no longer valid
  Q = Cancel
Your decision? 0
Enter an optional description; end it with an empty line:
> Demo for school assignment.
>
Reason for revocation: No reason specified
Demo for school assignment.
Is this okay? (y/N) y

You need a passphrase to unlock the secret key for
user: "Quenio C M dos Santos (Email Alternativo) <quenio@me.com>"
2048-bit RSA key, ID B03C59BB, created 2016-04-05


pub  1024D/DC26872D  created: 2002-03-16  expires: never       usage: SC
                     trust: full          validity: full
sub  2048g/4C24E598  created: 2002-03-16  expires: never       usage: E
[  full  ] (1). Ricardo Felipe Cust\xf3\x64io <custodio@inf.ufsc.br>

Save changes? (y/N) y

$ gpg --keyserver raxus.rnp.br --send-key dc26872d
gpg: sending key DC26872D to hkp server raxus.rnp.br

pub  1024D/DC26872D 2002-03-16            uid Ricardo Felipe Custódio <custodio@inf.ufsc.br>
sig  sig   DC26872D 2002-03-16 __________ __________ [selfsig]
sig  sig   1B58A0FA 2003-06-18 __________ __________ Andrei Luciano Krause <akrause@inf.ufsc.br>
sig  sig   C2CA87E1 2008-04-02 __________ __________ Pedro Henrique Ramos Ribeiro (Estudante - INE UFSC) <pedrohrribeiro@gmail.com>
sig  sig   AD816A4C 2012-10-05 __________ __________ Mauricio Simoes de Oliveira <mauricio.so@inf.ufsc.br>
sig  sig   51E08976 2012-10-09 __________ __________ Bruno Martinenghi Sidronio de Freitas (CCO UFSC) <brunosfreitas@gmail.com>
sig  sig   0909D07C 2016-04-12 __________ __________ Emmanuel Podesta Junior <epodesta158@gmail.com>
sig  sig   2B55081E 2016-04-12 __________ __________ Giovanni Antonio Tomaso Ferreira Rotta (Chave) <giovanni_rotta@hotmail.com>
sig  sig   E62976D7 2016-04-12 __________ __________ Ranieri Althoff (Key for INE5429) <ranisalt@gmail.com>
sig  sig   7F59BF09 2016-04-12 __________ __________ Luiz Henrique Urias de Sousa <luiz.urias@grad.ufsc.br>
sig  sig   F63A85C7 2016-04-12 __________ __________ Filipe G. Venancio (student) <filipenancio@gmail.com>
sig  sig   CFAFE5BD 2016-04-12 __________ __________ Guilherme Nakayama <guilherme.nakayama@hotmail.com>
sig  sig   B03C59BB 2016-04-12 __________ __________ Quenio C M dos Santos (Email Alternativo) <quenio@me.com>
sig  sig   2F3EE36E 2016-04-12 __________ __________ Lucas Finger Roman <lfrfinger@gmail.com>
sig  sig   7681F1FB 2016-04-12 __________ __________ Ion JosÃ© de Souza Neto <ionneto@gmail.com>
sig  sig   3546698C 2016-04-12 __________ __________ gilney nathanael mathias (none) <gilney_salvo@hotmail.com>
sig  sig   5D24C4C3 2016-04-12 __________ __________ Igor d. S. S. (.-. nova .-.) <gursol@yahoo.com.br>
sig  sig   D3032F08 2016-04-12 __________ __________ Cesar 2 (segunda identidade) <cesar.junior@grad.ufsc.br>
sig  sig   3BD39E4B 2016-04-12 __________ __________ Ana Cristina Dyonisio (SeguranÃ§a 2016.1) <anixmd@gmail.com>
sig  sig   FF971045 2016-04-12 __________ __________ AndrÃ© Azevedo Vargas (SeguranÃ§a da comp. 2016.1) <andre.azevedo.vargas@gmail.com>
sig  sig   5EF48040 2016-04-12 __________ __________ Gustavo Zambonin <gzmbnn@gmail.com>
sig  sig   B5E78288 2016-04-12 __________ __________ Eduardo Beckhauser (comentario da chave publica) <edubeckha@gmail.com>
sig  sig   C5C95A96 2016-04-13 __________ __________ Vinicius Couto Biermann <viniciusbiermann@hotmail.com>
sig  sig   572229E6 2016-04-13 __________ __________ Lucas Ribeiro Neis <lucasneis@hotmail.com.br>
sig  sig   0DC62EBB 2016-04-13 __________ __________ Willian de Souza <willianstosouza@gmail.com>
sig  sig   229D2744 2016-04-13 __________ __________ Jaime Mendes da Silva (Segunda Chave PrÃ¡tica SeguranÃ§a) <jaiminhosc@gmail.com>
sig  sig   6086792A 2016-04-13 __________ __________ Ana Cristina Dyonisio <anixmd@gmail.com>
sig  sig   B0721698 2016-04-13 __________ __________ Gustavo Jose Carpeggiani (NOVA) <g.j.carpeggiani@grad.ufsc.br>
sig  sig   2B004CD1 2016-04-14 __________ __________ Abraham Jean (New Key) <abramuus@hotmail.com>
sig revok  F63A85C7 2016-04-14 __________ __________ Filipe G. Venancio (student) <filipenancio@gmail.com>
sig revok  B03C59BB 2016-04-14 __________ __________ Quenio C M dos Santos (Email Alternativo) <quenio@me.com>sub  2048g/4C24E598 2002-03-16
sig sbind  DC26872D 2002-03-16 __________ __________ []
```

i) O que são os KeyIds dos certificados?

São números hexadecimais que identificam um certificado PGP. Derivados da parte final da "fingerprint" da chave pública, que é uma sequência relativamente curta de bytes gerada a partir da execução de um algoritmo de "hash" sobre a chave pública.

Podem ser usados para enviar atualizações de um certificado para um servidor de chaves e também encontrar certificados num servidor.

j) É possível prorrogar o prazo de validade de um certificado digital PGP?

Sim. É possível modificar a data de experação da chave "master" e também das sub-chaves.

No *gpg*, se utiliza-se o command `expire` para tanto.