

Segurança em Computação

Trabalho Individual 3

Adriano Tosetto - 15104099

30 de abril de 2019

1 Criação do Certificado

Antes de tudo foi necessário baixar o GPG. Para isso, foi executado o comando abaixo:

```
sudo apt-get install gpg
```

Após instalado, é necessário executar o comando:

```
gpg --gen-key
```

O GPG vai pedir algumas informações, como email e nome, então as chaves estarão disponíveis no local.

1.1 Backup da Private Key

Para realizar o backup da chave privada, o seguinte comando pode ser utilizado:

```
gpg --export-secret-keys KEYID > Desktop/private-key.asc
```

Onde o KEYID é identificador da chave.

1.2 Publicação da chave pública

Para mandar a chave para um servidor, o seguinte comando é necessário:

```
gpg --send-keys --keyserver <server> KEYID
```

onde `<server>` é o servidor para ser enviado, no meu caso foi <https://www.rnp.br>. KEYID é o id da chave. Também é possível mandar a chave diretamente no site do RNP <https://memoria.rnp.br/keyserver.php>

2 Assinaturas de Certificados e Revogação das Mesmas

2.1 Assinar o certificado de um terceiro

Antes de assinar o certificado de alguém, é necessário adicionar a chave dessa pessoa no anel de chaves. Para tal:

```
gpg --recv-keys KEYID
```

O KEYID é o id de chave da outra pessoa.

Para assinar essa chave, o seguinte comando é necessário:

```
gpg --sign-key KEYID
```

Onde KEYID é o id da chave da pessoa.

Agora é necessário enviar o certificado assinado para o servidor realizando o seguinte comando:

```
gpg --keyserver <server> --send-keys KEYID
```

Onde KEYID é o id da chave da pessoa e `|server|` é o servidor para onde se está mandando o certificado assinado.

Figura 1: Eu assinei o certificado do aluno Gustavo Olegário

```
pub 2048R/0F7EFC5D 2019-04-27
    Fingerprint=1869 394F 6819 38D4 3500 69CC D173 98B8 0F7E FC5D uid Gustavo Olegario <gustavo-olegario@hotmail.com>
sig sig3 0F7EFC5D 2019-04-27 2021-04-26 [selfsig]
sig sig 1F9CC988 2019-04-27 2021-04-26 Adriano Tosetto <adriano.rafael10@hotmail.com>
sig sbind 0F7EFC5D 2019-04-27 2021-04-26 [sub 4096R/7298483C 2019-04-27]
sig sbind 0F7EFC5D 2019-04-27 2021-04-26 [sub 2048R/7574F573 2019-04-27]
```

Para revogar a assinatura, utiliza-se o seguinte comando:

```
gpg --edit-key KEYID
```

Onde KEYID é o id da chave. Logo em seguida abre um terminal e é preciso entrar com o seguinte comando:

```
revsig
```

Ele vai pedir algumas informações (como o porquê da revogação) e só ir seguindo os passo. É preciso salvar a ação com:

```
save
```

Por fim, é preciso reenviar a chave para o servidor:

```
gpg --keyserver <server> --send-keys KEYID
```

Onde `|server|` é servidor (keyserver.cais.rnp.br, no meu caso) e KEYID é o id da chave.

Figura 2: Eu revoguei a assinatura do certificado do aluno Gustavo Olegário

```
pub 2048R/0F7EFC5D 2019-04-27
    Fingerprint=1869 394F 6819 38D4 3500 69CC D173 98B8 0F7E FC5D uid Gustavo Olegario <gustavo-olegario@hotmail.com>
sig sig3 0F7EFC5D 2019-04-27 2021-04-26 [selfsig]
sig sig 1F9CC988 2019-04-27 2021-04-26 Adriano Tosetto <adriano.rafael10@hotmail.com>
sig revok 1F9CC988 2019-04-27 2021-04-26 [sub 4096R/7298483C 2019-04-27]
sig sbind 0F7EFC5D 2019-04-27 2021-04-26 [sub 2048R/7574F573 2019-04-27]
sig sbind 0F7EFC5D 2019-04-27 2021-04-26 [sub 2048R/7574F573 2019-04-27]
```

3 Anel de Chaves Privadas

Há mais de uma chave privada no Anel. A primeira é a *Master Key* e sua principal função é identificar o usuário. É ela que é usada para assinar o nome e email do usuário no certificado. As outras chaves no anel são as *subkeys*. Elas são usadas para encriptar e assinar dados reais. A *Master Key* assina as *subkeys* para mostrar que elas pertencem ao usuário.

A ideia desse esquema é fazer com que o gerenciamento de chaves se torne mais fácil. Com ele é possível substituir as *subkeys* e outro ponto é que a *Master Key* fica muito menos exposta.

4 Assinatura Local e em Servidor

5 Banco de Dados de Confiabilidade

6 Sub-chaves

As sub-chaves, como dito anteriormente, servem para facilitar o gerenciamento e dar mais segurança ao usuário GPG. Elas estão associadas ao trabalho de assinar documentos reais e funções de encriptação. Elas devem ser assinadas pela *Master Key* para que elas sejam confiáveis. Elas podem ser revogadas com relativa facilidade também devido a esse esquema.

7 Certificado GPG

8 Envio de Arquivo Cifrados com GPG

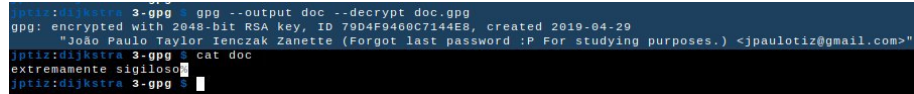
Para encriptar usando o GPG, primeiro é preciso importar a chave para o local. No meu caso, usarei a chave pública do aluno *João Paulo Tiz* com o comando:

```
gpg --keyserver keyserver.cais.rnp.br --recv DCAE898A
```

Para encriptar:

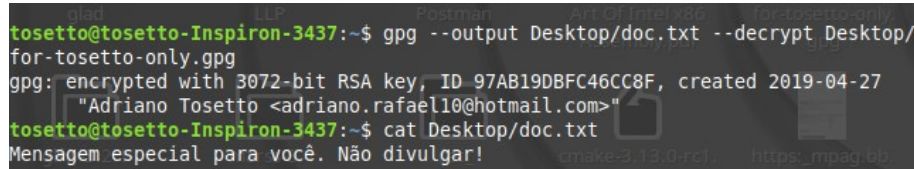
```
gpg --output doc.gpg --encrypt --recipient DCAE898A doc
```

Figura 3: Tela do computador do Tiz após decifrar o arquivo cifrado que eu mandei



```
jptiz@dijkstra 3-gpg $ gpg --output doc --decrypt doc.gpg
gpg: encrypted with 2048-bit RSA key, ID 79D4F9460C7144E8, created 2019-04-29
"João Paulo Taylor Ienczak Zanette (Forgot last password :P For studying purposes.) <jpaulotiz@gmail.com>"
jptiz@dijkstra 3-gpg $ cat doc
extremamente sigiloso
jptiz@dijkstra 3-gpg $
```

Figura 4: Tela do meu computador após eu decifrar uma mensagem que o Tiz me enviou usando minha chave pública



```
tosetto@tosetto-Inspiron-3437:~$ gpg --output Desktop/doc.txt --decrypt Desktop/for-tosetto-only.gpg
gpg: encrypted with 3072-bit RSA key, ID 97AB19DBFC46CC8F, created 2019-04-27
"Adriano Tosetto <adriano.rafaell10@hotmail.com>"
tosetto@tosetto-Inspiron-3437:~$ cat Desktop/doc.txt
Mensagem especial para você. Não divulgar!
tosetto@tosetto-Inspiron-3437:~$
```

9 Assinatura Anexada & Assinatura Separada

9.1 Assinatura Anexada

9.2 Assinatura Separada