Leonardo Schlüter Leite

# SEGURANÇA EM COMPUTAÇÃO: TRABALHO INDIVIDUAL 3

Florianópolis

2019

**SUMÁRIO**

# 1 RESPOSTAS

## 1.1 QUESTÃO 1

Foram utilizados os seguintes comandos em bash, no terminal do Ubuntu 18.04. Estes comandos foram retirados do site fornecido https://help.ubuntu.com /community/GnuPrivacyGuardHowto

```
1. gpg --gen-key //aqui foram inseridos as infos
   necessarias para criar o certificado e a
   chave
2. export GPGKEY=62E6B6A3
3. gpg -armor --export leonardoschluter@gmail.com
   > mykey.asc // utilizado para exportar minha
   chave publica
```

O Resultado destes comandos foi um certificado(leonardoschluter@gmail.com), uma chave privada, uma chave pública(KeyID: 62E6B6A3) e o arquivo mykey.asc. O conteúdo deste arquivo foi depois utilizado para publicar o certificado no Servidor de chaves PGP do CAIS.

## 1.2 QUESTÃO 2

Até a etapa de publicar o certificado criado o processo é o mesmo da questão anterior. Sendo que agora o KeyID é 9229C802, o email utilizado permanece o mesmo. Agora, para criar o certificado de revogação, importá-lo e depois publicar no servidor de chaves PGP do CAIS foram utilizados os seguintes comandos em bash, no terminal do Ubuntu 18.04:

```
1. gpg -o certificado_revogado.asc --gen-revoke -
   armor 9229C802
2. gpg --import certificado_revogado.asc
3. gpg --keyserver keyserver.cais.rnp.br --send-
   keys 9229C802
```

A Figura 1 mostra o resultado da questão 1 e 2.

Figura 1 – KeyIDs geradas no servidor de chaves PGP do CAIS.

```
Type bits/keyID     Date       User ID
```

```
pub  3072R/9229C802 2019-04-23 *** KEY REVOKED *** [not verified]
                               Schluter Teste Trabalho 3 <leonardoschluter@gmail.com>
```

```
pub  3072R/62E6B6A3 2019-04-23 Leonardo SchlÃ¼ter Leite <leonardoschluter@gmail.com>
```

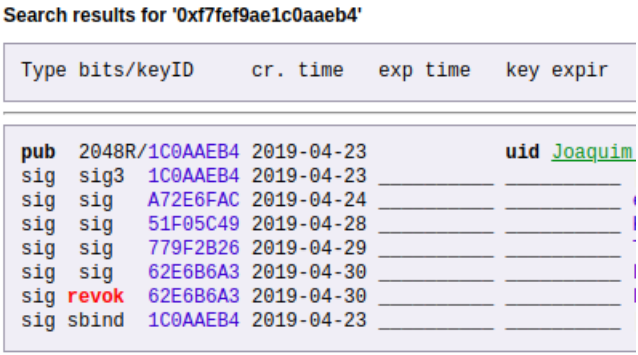
## 1.3 QUESTÃO 3

Primeiro é necessário assinar algum certificado. Para este exemplo usaremos o KeyID 1C0AAEB4 do colega Joaquim Boschini. Para realizar a assinatura do certificado, primeiro precisamos baixar a chave, importá-la, depois realizar a assinatura e enviar novamente para o servidor de chaves(o ideal é mandar a assinatura para o dono da chave, para que o mesmo possa publicá-la).Para isso foi utilizado os seguintes comandos em bash:

1. gpg --recv-keys 0x1C0AAEB4
2. gpg --fingerprint 1C0AAEB4 // utilizado para verificar se realmente eh o certificado que eu queria
3. gpg --sign-key 1C0AAEB4
4. gpg -o joaquimSigned.asc --armor --**export** 1C0AAEB4
5. gpg --keyserver keyserver.cais.rnp.br --send-keys 1C0AAEB4

Depois para revogar a assinatura no certificado do colega, utilizamos o comando gpg –edit-key, que permite a execução de alguns comandos próprios. Dentro do ambiente do edit-key utilizamos o comando >revsig para justamente revogar a assinatura e o comando >save para, obviamente, salvar. Depois disso publicamos a revocação utilisando o comando –send-keys. Podemos observar na figura 2 que o certificado foi assinado pela minha chave (KeyID 62E6B6A3) e depois a assinatura foi revogada.

Figura 2 – Assinaturas do KeyID 1C0AAEB4




## 1.4 QUESTÃO 4

Um anel de chaves privadas é, segundo a wiki do GNOME, uma coleção de componentes que guarda senhas, chaves, certificados e disponibiliza o que está guardado com outras aplicações. o Anel de chaves do GNOME é implementado para seguir o padrão PKCS#11, que define como chaves e certificados devem ser manejados. O Keyring no ubuntu fica localizado em .local/share/keyrings. Teoricamente apenas o usuário que criou o keyring tem acesso. Este acesso se dá através de sessão.

## 1.5 QUESTÃO 5

Assinar localmente faz com que apenas o meu keyring contenha esta assinatura para a chave x. Enquanto assinar no servidor replica para todos os outros servidores GPG, assim replicando a assinatura para todas as replicas online.

## 1.6 QUESTÃO 6

## 1.7 QUESTÃO 7

Subchaves são como as chaves normais, porém está ligada à um par de chave mestre, segundo a wiki do Debian.Porntato, pode-se usá-las como as chaves normais. Servem principalmente para evitar que você utilize seu par de chaves mestre para coisas do dia a dia. Assim evitando que: se algo aconteça à chave que você usa no dia a dia, você não perca sua identidade online, já que seu par de chaves mestre é tudo, no mundo online.

## 1.8 QUESTÃO 8

Para adicionar uma foto à chave, utilizamos o comando gpg –edit-key, que permite a execução de alguns comandos próprios. Dentro do ambiente do edit-key utilizamos o comando >addphoto, então informar o endereço da imagem desejada. Após feito isso, basta salvar e enviar novamente a chave para o servidor de chaves.

## 1.9 QUESTÃO 9

## 1.10 QUESTÃO 10

Para tornar sigiloso ao público um arquivo txt, por exemplo, basta que você tenha acesso a chave pública do destinatário. Tendo essa chave pública, basta executar um comando em bash:

```
1. gpg --output arquivoExemplo.txt.gpg --encrypt
   --recipient meu.colega.deturma@ufsc.br.com
   arquivoExemplo.txt
```

Depois, basta enviar o arquivExemplo pela internet e o outro lado vai conseguir descriptografar utlizando o seguinte comando:

```
1. gpg --output arquivoExemplo.txt --decrypt
   arquivoExemplo.txt.gpg
```

## 1.11 QUESTÃO 11

Para assinar um documento, é um tanto quanto fácil através do terminal. Basta usar o comando "gpg –output arquivoExemplo.sig –sign arquivoExemplo". Para assinar sem anexar ao documento, basta adicion "detach-"na frente do "sign", assim:"gpg –output arquivoExemplo.sig –detach-sig arquivoExemplo".

Agora para verificar é mais fácil ainda, quando for uma assinatura no próprio documento, basta usar o comando: gpg –verify arquivoExemplo.sig. Se for uma assinatura separada do documento, basta informar os dois arquivos, o da assinatura e o do documento, assim: gpg –verify arquivoExemplo.sig arquivoExemplo