Trabalho 3 - PGP

Vinicius Macelai

October 2019

1

Foi gerado o certificado PGP, segue a chave pública como prova:

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
mQMuBF2bNe8RCADjlod8zM2M+TBVKQ386L+X3f0ZCkcAM7luEvrLCEPMFXPvoT6l
JpJqsb76Zgw+MMv+Sv9nBBoUw9WvG9TcJl82VcE+3UYqOzTrj2FJlR0vKl8FqhHp
8o9NHcII/68GXQ4ofNKMwOwh/+ghIhDaDnKU4TmV/xFom4qMjpPmM3uuAKMoxHUW
tzW4g/9ut5Jo7Har3fAUKIZI46Lx7N0ZXYLr8JgnMzjBQjlG4cs4rTfx2L2hJgB2
qrUM0apNHb80du6/i9rlYS9ZC8XM1g1WZYiSQD5w6yYNA5a4+j6Z/qcIMqA5G/8O
rs79f55ny4W7vgRJBAfqNMyZSOE07obu9F7bAQCFRaHBkSfYZR+pmc/0lmpaOiss
VQARMtvVgvNDCOm+dwf/Q24OhB4DCfo7hZfR39IIpfu3X++MYjPmgBQy2UI1UpCq
eOPabPpYBCcMrIY22NBXSGLgYqeMYuoKMgUSIzryfXRt4m42amMRo4Jm5gdGA7xe
4T1Z2k6AlIOTnGVnWBdHgiOsLkk2ZLjfpDbYGOBI84qyi8ibwdPor4ZC569U6jPC
CJWuqI1Za/zEeAxY4NwCOb/3f94p7POjjSvWYhMr4Nk95e/oFxVmPXm5UNhv2j7s
/doxGYVheWad4ORvy1XI2PlIqz0dpFD392nhqqJKMhBNZMHkT/lpLpW2QL9nVTWz
ourJqVtDyIN052aVeceiZOT+AQajArzPJ0h96FpS7wf+N5jef2bshWVMUmzdv09a
XLK0ceUnhF1/ckGnfmdhJ2ue/RZsSRdJzfQJjlt/foJR6uqqq9vLJfLd2GnWUFkQ
IYh8oK5h0pUMLp0y557sJAIKR6QhlF0y5CyK6olDgfyrJB7kfwRldQnlYKTdvvpZ
Mgi1zGowfgVQbj3akMwEtpIVbAIHzrtoajRCLwrd+LxtxlbbssRM5OkACALTHdhT
kBVPC6qEyal2pGXtutMnURCdoxPTI7Iokp6IAzJSguPtwhfrmhJ2AWHh13RWEC84
E8km4V63zCT+GncSjzSqPl0L3gbOPuZUfg1Mv63cCK0WmllZtVyTvAcit9qcfg93
yrRGVmluaWNpdXMgTWFjZWxhaSAoVHJhYmFsaG8gZGUgc2VndXJhbsOnYSkgPHZp
bmljaXVzLm1hY2VsYWlAZ21haWwuY29tPoiQBBMRCAA4FiEE3fP2o4buG1rNI7G+
hd2Noqo7nucFAl2bNe8CGwMFCwkIBwIGFQoJCAsCBBYCAwECHgECF4AACgkQhd2N
oqo7nudDwAD8Cn+saBEjo+78sXQC0cGzi0/Ma7zkN2Z+Vb0id41k/N0A/AoGfa2z
HgcH2aFBbZflph4sVbuQcjU1Ra1S+f/Aid6M
=wC0y
-----END PGP PUBLIC KEY BLOCK-----
```

A chave pública foi publicado no repositório Keyserver PGP(https://keyserver.pgp.com/)

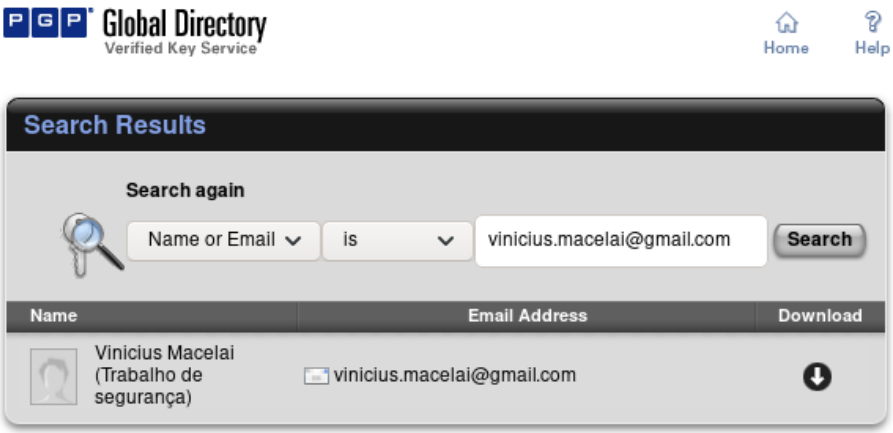

Figure 1: Keyserver PGP

2 e 3

Foi criado então o certificado de revogação do certificado criado:

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Comment: This is a revocation certificate

iHgEIBEIACAWIQTd8/ajhu4bWs0jsb6F3Y2iqjue5wUCXZs6jgIdAAAKCRCF3Y2i
qjue5wCFAP9lX7PilNYQROisiGqD508jhvoVZrTw2aFO5cSN9SxJNQD/RHPstBYm
KROSnyndxcGZOrZjuxlOOZBnhDkVfCPyOcs=
=pGT7
-----END PGP PUBLIC KEY BLOCK-----
```

4

PGP foi pensado para que os proprietários das chaves, mantêm e distribuem os key rings de seus certificados. Intuitivamente, os keys rings são formados por mais de uma chave. A primeira chave é chamada de master key, como é a principal, ela é usada apenas para identificar o proprietário da chave, ou seja, ela assina o nome do usuário e o email incluido no certificado.

Como eu gerei a chave localmente, o anel de chaves vai estar armezenado em meu computador. Somente o proprietário deve ter acesso, visto que são as chaves privadas.

5

O ato de se assinar uma chave no mundo PGP, quer dizer que você confia em uma chave. A pergunta da a entender que a assinatura é feito por um servidor, pois não achei nada que dizia que uma chave privada PGP possa ser enviada a um servidor. Então se entende que o servidor está assinando uma chave como confiável e por consequência se algum usuário confia no servidor irá confiar nesta chave. De forma que se fosse assinado localmente, apenas naquele computador a chave seria confiável.

6

O banco de dados de confiabilidade é organizado de forma que há vários níveis de de confiança, então haverá chaves com maior confiança e outras com menos, dependendo do nível que você da a uma determinada chave e se outras chaves que você confia assinarem uma outra, você terá um certo nível de confiança nesta também. Segue a estrutura:

- **(-)** Nenhuma confiança do proprietário atribuída / ainda não calculada.
- **(e)** O cálculo da confiança falhou; provavelmente devido a uma chave expirado.
- **(q)** Não há infomrações suficientes para determinar.
- **(n)** Nunca confiar nesta chave.
- **(m)** Marginalmente confiável.
- **(f)** Totalmente confiável.
- **(u)** Ultimate confiável(chave do dono).

7

As outras chaves do key ring, que não são a primária. Essas chaves são chamadas de subkeys, elas que são usadas para cifrar ou assinar dados na realidade. A chave mestra assina essas outras chaves para provar que elas pertencem ao mesmo certificado e que são tão confiáveis quanto a chave mestra.

9

Existem diversas implementações de softwares que fazem o papel de um key-server, são redigidos pela RFC 2440[1]. Utilizam de HKP(OpenPGP HTTP Keyserver Protocol) ou HKPS para sua versão segura com TLS.

Já para a parte de sincronização, deve-se utilizar do Synchronizing OpenPGP Key Server (SKS) no seu servidor. Também redigido pela RFC 2440.

10

Para tornar um arquivo sigiloso, basta assina-lo, irá produzir uma saída como esta:

Figure 2: Texto cifrado

Da forma que a mensagem original pode ser conseguida com a operação inversa. Obtendo o resultado original que a mensagem era "sec"

Figure 3: Texto decifrado

11

Realizando o processo de assinatura e verificação da assinatura.

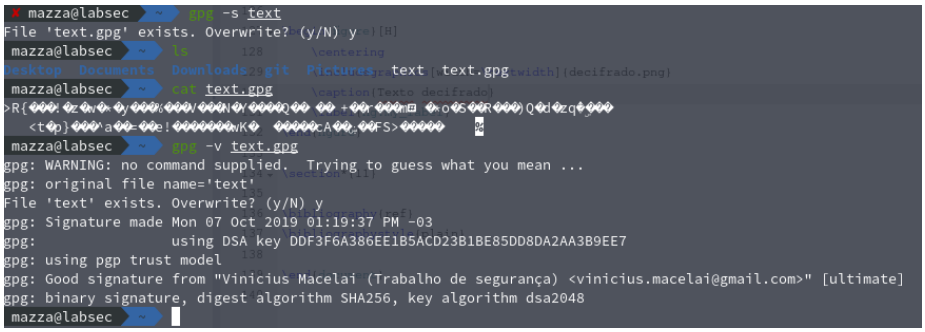

Figure 4: Assinatura e verificação

References

[1] Hal Finney, Rodney L. Thayer, Lutz Donnerhacke, and Jon Callas. OpenPGP Message Format. RFC 2440, November 1998.