Segurança em Computação: Trabalho PGP

Rafael Begnini de Castilhos (20205642)

21 de junho de 2022

Resumo

O presente trabalho possui como objetivo praticar e analisar o uso de PGP.

Sumário

1 Questão 1

Para cumprir a primeira parte do trabalho, criou-se um par de chave pública/privada. Para criar esse par de chaves, seguiu-se o tutorial disponibilizado. As secções utilizadas desse guia foram: *Generating an OpenPGP Key, Setting the key to be the default, Adding Encryption Capabilities, Creating a revocation certificate, Making an ASCII armored version of your public key.*

O Key id gerado foi: 47D6A8FF.

Após gerar o par de chaves, foi acessado o site da RNP. Com o conteúdo de mykey.asc copiado, colou-se o mesmo na caixa de conteúdo da secção *Submissão de chaves* e clicou-se no botão enviar. Fez-se, em seguida, uma busca por chave através do e-mail para garantir de que a chave havia sido cadastrada, conforme imagem apresentada abaixo.

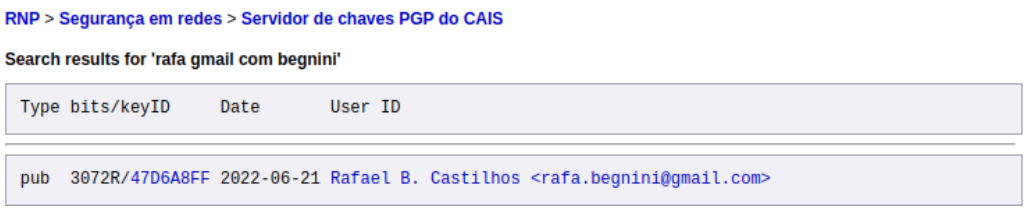

Figura 1: Busca por chave válida.

2 Questão 2

Foi realizado o mesmo procedimento de criação exemplificado na questão 1, apenas alterando o e-mail.

O Key id gerado foi: E3318008.

Para revogar o certificado de testes, seguiu-se os comandos da secção *Não tenho o certificado de revogação*, no próprio site da RNP, para revogar a chave enviada. Para garantir que o processo havia sido executado com sucesso, procurou-se novamente a chave através do e-mail e pode ser constatado, como mostra a imagem abaixo, que tudo havia ocorrido como esperado.

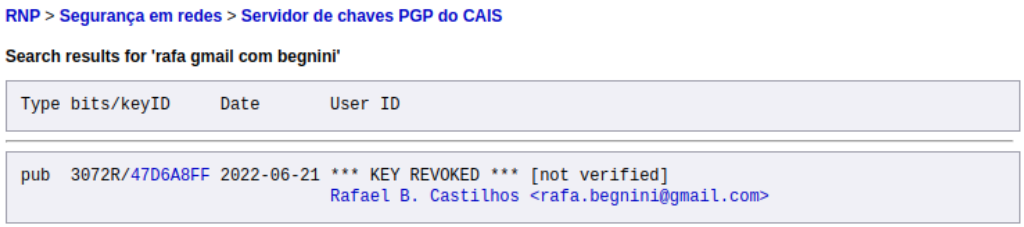

Figura 2: Busca por chave revogada.

3 Questão 3

A assinatura de um certificado inicia pela identificação do Key id da outra pessoa. Neste caso, será assinado a chave com Key id igual à 0x27958a6b8011793a. Primeiro é recuperado as chaves:

gpg –keyserver keyserver.cais.rnp.br –recv-keys 0x27958a6b8011793a

Figura 3: Recupera chaves.

Depois é assinado o certificado:

gpg –keyserver keyserver.cais.rnp.br –sign-key 0x27958a6b8011793a

```
pub  rsa4096/27958A6B8011793A
     created: 2022-06-20  expires: 2024-06-20  usage: SC
     trust: unknown       validity: unknown
sub  rsa4096/DEB6D0207CD58724
     created: 2022-06-20  expires: 2024-06-20  usage: E
[ unknown] (1). Arthur Moreira Rodrigues Alves <arthur.mra@grad.ufsc.br>
[ unknown] (2)  [jpeg image of size 5120]

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

pub  rsa4096/27958A6B8011793A
     created: 2022-06-20  expires: 2024-06-20  usage: SC
     trust: unknown       validity: unknown
 Primary key fingerprint: 135E 07B9 1752 5774 B1A7  2F81 2795 8A6B 8011 793A

     Arthur Moreira Rodrigues Alves <arthur.mra@grad.ufsc.br>
     [jpeg image of size 5120]

This key is due to expire on 2024-06-20.
Are you sure that you want to sign this key with your
key "Rafael B. Castilhos <rafael.castilhos@grad.ufsc.br>" (8A1D5763E3318008)

Really sign? (y/N) y
```

Figura 4: Assinatura no certificado.

E então envia a assinatura para o servidor RNP:
gpg –keyserver keyserver.cais.rnp.br –send-keys 0x27958a6b8011793a

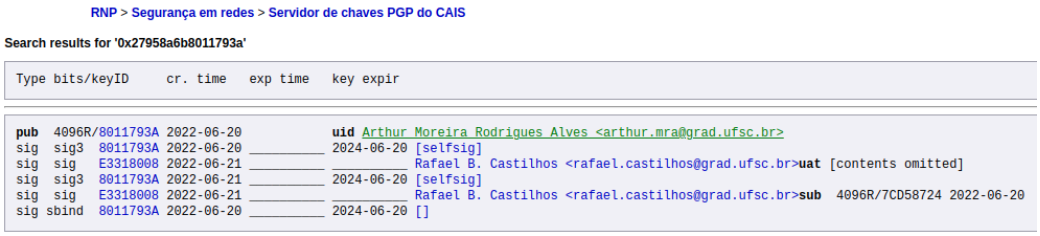

Figura 5: Certificado assinado no servidor RNP.

Com intenção de revogar a assinatura realizada no certificado, os comandos que utilizados foram:
gpg –edit-key 0x27958a6b8011793a
revsig
save
gpg –keyserver keyserver.cais.rnp.br –send-keys 0x27958a6b8011793a

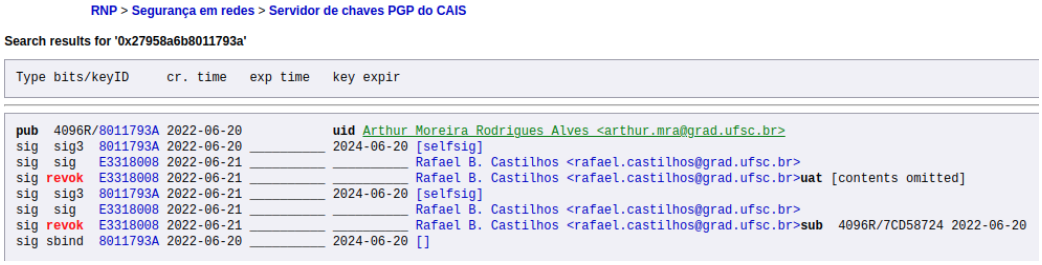

Figura 6: Certificado revogado no servidor RNP.

4 Questão 4

Um anel de chave consiste em uma chave pública e sua chave privada correspondente, ambas necessárias para descriptografar os dados. Cada usuário mantém duas estruturas de dados de porta-chaves: um chaveiro privado para seus próprios pares de chaves pública/privada e um chaveiro público para as chaves públicas correspondentes. São armazenadas no diretório /.gnupg.

Os proprietários das chaves retêm e transmitem os chaveiros em seus certificados. A primeira chave é chamada de chave mestra e seu uso principal é agir como a identidade do proprietário. Outras chaves incluídas no anel de chaves são chamadas de sub-chaves. A chave mestra assina as sub-chaves como uma prova de que elas realmente pertencem ao certificado e são tão confiáveis quanto a chave mestra [2].

O anel de chave é uma tabela contendo as seguintes informações:

- Data e hora de quando o par foi gerado;
- ID da chave (composto por 64 dígitos menos significativo da chave pública);
- A parte pública da chave;
- A parte privada criptografada;
- ID do usuário.

5 Questão 5

Quando o usuário cria as chaves, ele poderá assiná-la localmente com sua própria chave privada para confiar nela. Ao assinar localmente as chaves, a confiança na chave permanecerá puramente local em seu sistema e não se tornará parte da rede de confiança. Ou seja, ao assinar uma chave e enviar a assinatura para o servidor o usuário confia que a chave assinada é verdadeira [3].

6 Questão 6

O usuário distribui sua chave pública fornecendo-a pessoalmente aos seus correspondentes. Entretanto, as chaves s˜ao frequentemente distribuídas por e-mail ou algum outro meio de comunicação eletrônico.

Uma chave pública recebida pelo servidor é adicionada ao banco de dados do servidor ou mesclada com a chave existente, se já estiver presente. Quando uma solicitação de chave chega ao servidor, o servidor consulta seu banco de dados e retorna a chave pública solicitada, quando encontrada.

Usando um servidor de chaves torna o processo mais fácil. Quando Beto assina a chave de Alice, ele envia a chave assinada para o servidor de chaves. O servidor principal adiciona a assinatura de Beto à sua cópia da chave de Alice. Indivíduos interessados em atualizar sua cópia da chave de Alice, consultam o servidor de chaves por iniciativa própria para recuperar a chave atualizada. Com isso, Alice nunca precisa se envolver com distribuição e pode recuperar assinaturas em sua chave simplesmente consultando um servidor de chaves [1].

Portanto conclui-se que quanto mais assinaturas um certificado possuir, mais confiável ele será.

7 Questão 7

As sub-chaves são chaves adicionais e são como as chaves públicas e privadas, exceto pelo fato de estarem ligadas ao par de chaves mestra. A parte útil das sub-chaves é que elas podem ser usadas para assinatura ou criptografia, além disso podem ser revogadas independentemente das chaves mestras.

Sub-chaves são outras chaves no anel, utilizadas para assinar e encriptar dados reais. A chave-mestra assina as sub-chave para informar que estas

pertencem ao usuário.

8 Questão 8

Com a finalidade de adicionar sua imagem à sua chave PGP, será utilizado os seguintes comandos: *gpg –edit-key E3318008*

addphoto

Neste momento é necessário informar o caminho até a imagem ou foto. Em meu caso, foi: "/home/rafaelbcastilhos/Downloads/orange.jpeg"

Após isso é possível salvar e continuar.

save

gpg –send-keys –keyserver keyserver.cais.rnp.br E3318008

9 Questão 9

Um servidor de chaves necessita da execução do protocolo *Synchronizing OpenPGP Key Server (SKS)*. A implementação desse servidor de chaves usa um algoritmo de reconciliação eficiente e confiável para manter o banco de dados em sincronia com outros servidores SKS.

10 Conclusão

Realizando esse trabalho foi possível colocar em prática os tópicos apresentado em sala de aula sobre PGP e Assinatura em certificados digitais, fazendo referência as possíveis abordagens na área da segurança da computação. Em suma, o trabalho cumpriu seus requisitos pedagógicos e didáticos para a formação de um profissional da ciência da computação.

Referências

[1] M. Copeland. The gnu privacy handbook: Chapter 3. key management. `https://www.gnupg.org/gph/en/manual/x457.html"`, year=2022, note =.

[2] Imaeses. Understanding key rings. `http://www.imaeses.nl/KeyRing/What_is_PGP.html`, 2022. [Online; acessado em 21 de junho].

[3] ReviewBoard. Pgp signatures. https://www.reviewboard.org/downloads/pgp-signatures", year=2022, note =.