Trabalho PGP

Pedro Henrique Aquino Silva
Matrícula: 18102719

1. Criei chave PGP com “gpg --full-gen-key”:
   - Opção 1: RSA and RSA
   - Default bit size: 3072 bits
     `"Pedro Henrique Aquino Silva ("Chave criada para trabalho de Segurança em Computação") <pedro.aquino@grad.ufsc.br>"`
   - Chave adicionada ao keyserver do Ubuntu em https://keyserver.ubuntu.com com KeyID `342B9B91A0ED6E24`
2. Chave nova criada para testar revogação:

   Search results for 'PedroTeste'

   ```
   Type bits/keyID            cr. time   exp time   key expir
   ```

   ```
   pub rsa3072/2f492fa343bb4898c63e70729fb3f6a6f356b6ca 2022-07-08T23:13:57Z
           Hash=b152ae936fdad4eff1728f1d407d469e

   uid PedroTeste <pedro.aquino@grad.ufsc.br>
   sig  sig  9fb3f6a6f356b6ca 2022-07-08T23:13:57Z 2024-07-07T23:13:57Z ____________________ [selfsig]

   sub rsa3072/429f9351875f1abc218ad6aead17e36c01b00e77 2022-07-08T23:13:57Z
   sig sbind 9fb3f6a6f356b6ca 2022-07-08T23:13:57Z ____________________ 2024-07-07T23:13:57Z []
   ```

   Depois revogado:

   ```
   pub rsa3072/2f492fa343bb4898c63e70729fb3f6a6f356b6ca 2022-07-08T23:13:57Z
           Hash=c38b8294790151a791a343e8ced5da1b
   sig revok 9fb3f6a6f356b6ca 2022-07-08T23:18:20Z ____________________ ____________________ [selfsig]

   uid PedroTeste <pedro.aquino@grad.ufsc.br>
   sig  sig  9fb3f6a6f356b6ca 2022-07-08T23:13:57Z 2024-07-07T23:13:57Z ____________________ [selfsig]

   sub rsa3072/429f9351875f1abc218ad6aead17e36c01b00e77 2022-07-08T23:13:57Z
   sig sbind 9fb3f6a6f356b6ca 2022-07-08T23:13:57Z ____________________ 2024-07-07T23:13:57Z []
   ```

3. Foi realizada assinatura da chave do colega Teo Haeser Gallarza, que também assinou a minha chave. Logo após, foi feita a revogação da assinatura. Acidentalmente, foram realizadas duas revogações da mesma assinatura.

```
pub rsa3072/41b54a44ff487e85bf4c85e7d722149e881c371d 2022-07-08T22:48:23Z
        Hash=2fe926ed9e5dc8d81f28b63fb2b45c76

uid Teo H G <teogallarza@hotmail.com>
sig  sig  d722149e881c371d 2022-07-08T22:48:23Z 2024-07-07T22:48:23Z _____________________ [selfsig]
sig  sig  342b9b91a0ed6e24 2022-07-08T23:29:01Z _____________________ _____________________ 342b9b91a0ed6e24
sig revok 342b9b91a0ed6e24 2022-07-08T23:43:29Z _____________________ _____________________ 342b9b91a0ed6e24
sig revok 342b9b91a0ed6e24 2022-07-08T23:47:26Z _____________________ _____________________ 342b9b91a0ed6e24

sub rsa3072/f170fe37704b188dcde1195ba9429a041de85ec2 2022-07-08T22:48:23Z
sig sbind d722149e881c371d 2022-07-08T22:48:23Z _____________________ 2024-07-07T22:48:23Z []
```

4. O anel de chaves privadas é um arquivo que contém as chaves privadas. O anel se encontra no diretório ~/.gnupg quando usando a aplicação GnuPG. Esse porta chaves deve ser possível de ser acessado somente pelo dono das chaves.
5. Assinar localmente faz com que levemos em conta na assinatura somente as informações disponíveis na máquina da assinatura. Ao assinar no servidor, ou sincronizar com o servidor, as informações são propagadas na rede de confiança.
6. A confiabilidade deste banco de dados é descentralizado, utilizando o conceito de “web of trust”. As implementações de OpenPGP envolvem um mecanismo de votação para determinar para o usuário quem é confiável ao utilizar PGP.
7. Subchaves são chaves criadas e associadas a uma chave principal. São formas de facilitar a organização e manutenção de chaves, e podem ser utilizadas para assinar ou criptografar mensagens de forma independente da chave principal.
8. A foto foi inserida localmente por meio de “gpg --edit-keys” e foi adicionada uma foto localmente. Contudo, pela foto ser demasiado grande, e possivelmente devido ao formato empregado, ela não pode ser visualizada no servidor de chaves. Segue um print da saída local de “gpg --list-keys”, com oa imagem .jpeg inserida:

```
/home/pedro/.gnupg/pubring.kbx
------------------------------
pub   rsa3072 2022-07-02 [SC]
      2C1FDC23B841FC1662937C5D342B9B91A0ED6E24
uid           [ultimate] Pedro Henrique Aquino Silva (Trabalho para disciplina de Segurança em Computação) <pedro.aq
uino@grad.ufsc.br>
uid           [ultimate] [jpeg image of size 44145]
sub   rsa3072 2022-07-02 [E]
```

9. Existem diversas soluções disponíveis. Uma delas é utilizar a ferramenta sks-keyserver, que cuida da sincronização com os demais servidores. É uma ferramenta eficiente para a reconciliação de dados e resolução de conflitos.
10. (não feito)
11. (não feito)