

Oficina de GNUPG com festa de assinatura de chaves



Antes da festa

- Gere o seu par de chaves
- Gere o certificado de revogação
- Publique a sua chave pública
- Imprima cartões com as informações da sua chave pública
- Leve os cartões para a festa

Durante a festa

- Troque os cartões que você trouxe com os outros participantes
- A cada troca de cartão, confira criteriosamente os documentos oficiais com foto do dono do cartão
- Marque com uma caneta os cartões recebidos que você conferiu os documentos
- Guarde os cartões recebidos para usá-los depois da festa
- Importante: não leve tequila para a festa :-)

Depois da festa

- Para cada cartão recebido e cujos documentos você conferiu:
 - Obtenha uma cópia da chave pública
 - Assine-a com a sua chave privada
 - Retorne a chave assinada por e-mail, ou publique-a
- Importe as assinaturas que você receber por e-mail e publique-as
- Atualize seu chaveiro com as novidades dos servidores de chaves
- Defina o seu grau de confiança nos donos das outras chaves

Configuração (opcional)

- Configure o gnupg para usar o servidor de chaves da festa, adicionando no arquivo `~/.gnupg/gpg.conf`:
 - `keyserver hkp://servidor_de_chaves`

Antes da festa

Gere o seu par de chaves

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

Gere o certificado de revogação

```
gpg --output revoke.asc \  
--gen-revoke $CHAVE
```


Publique a sua chave pública

```
gpg --send-keys $CHAVE
```

Imprima os cartões

```
gpg --fingerprint $CHAVE
```

Durante a festa

- Troque os cartões que você trouxe com os outros participantes
- A cada troca de cartão, confira criteriosamente os documentos oficiais com foto do dono do cartão
- Marque com uma caneta os cartões recebidos que você conferiu os documentos
- Guarde os cartões recebidos para usá-los depois da festa
- Importante: não leve tequila para a festa :-)

Depois da festa

Obtenha a chave pública

```
gpg --recv-keys $CHAVE
```

Assine a chave

```
gpg --sign-key $CHAVE
```

Retorne a chave assinada por
e-mail...

```
gpg --armor \  
--output chave.asc \  
--export $CHAVE
```

...ou publique a chave assinada

```
gpg --send-keys $CHAVE
```


Importe as assinaturas recebidas
por e-mail e publique-as

```
gpg --import $CHAVE.asc
```

```
gpg --send-keys $CHAVE
```

Atualize o seu chaveiro

```
gpg --refresh-keys
```

Defina o seu grau de confiança nos donos das outras chaves

```
gpg --update-trustdb
```

Referências

- <http://gnupg.org/gph/en/manual.html>
- http://www.cryptnet.net/fdp/crypto/keysigning_party/en/keysigning_party.html
- <http://xkcd.com/364/>

Sobre

- Contato:
adrianorg@arg.eti.br
<http://arg.eti.br/>
- Licença:
<http://creativecommons.org/licenses/by-sa/3.0/>



Log

- 09/04/2011: FLISOL, NH
- 17/09/2011: Dia da Liberdade de Software, NH
- 19/11/2011: IV Festival de Software Livre do Vale do Sinos, NH
- 28/04/2012: FLISOL, NH
- 28/09/2013: Dia da Liberdade de Software, NH
- 19/09/2015: Dia da Liberdade de Software, NH