Usando o GnuPG

De Eriberto Wiki

Esta página está em construção e deverá estar pronta em poucos dias. Por favor, volte depois ou consulte-a agora com cautela e paciência.

by (C) João Eriberto Mota Filho (http://www.eriberto.pro.br) <eriberto (a) eriberto pro br>

Siga-me no twitter
http://twitter.com/eribertomota

Artigo criado em: 15 de abril de 2007.

Última atualização: veja o rodapé desta página.

Tiny URL ou bit.ly: http://bit.ly/GNUPG

Este artigo é um tutorial para as pessoas que desejam conhecer e utilizar o GPG.

Índice

O PGP (Pretty Good Privacy) e o GnuPG (GNU Privacy Guard ou GPG)

O Pretty Good Privacy (Privacidade Muito Boa) é um sistema de criptografia assimétrica e assinatura digital, desenvolvido em 1991 por Philip Zimmermann. No início, o PGP possuia restrições quanto ao uso. Assim sendo, o Projeto GNU (http://www.gnu.org) desenvolveu o GnuPG (GNU Privacy Guard), que é totalmente compatível com o PGP. O GnuPG segue as especificações do protocolo OpenPGP, definido pela RFC 2440 (http://www.faqs.org/rfcs/rfc2440.html).

O site do PGP é o http://www.pgp.com. O site do GnuPG (GPG) é o http://www.gnupg.org.

Instalação no Debian GNU/Linux

O GnuPG poderá ser instalado com o comando:

```
# apt-get install gnupg
```

O chaveiro digital

O chaveiro digital de um usuário é a reunião de todas as chaves de interesse de tal usuário. Esse chaveiro, geralmente, contém o par de chaves do usuário e as chaves públicas de outros usuários. O chaveiro digital de cada usuário fica armazenado em *~/.gnupg* e pode ser visto com o comando:

```
$ gpg --list-keys
```

É possível que um usuário tenha mais de uma chave, principalmente se as mesmas tiverem tamanhos diferentes (em bits). A diferença poderá ser vista no ID das mesmas.

Cada chave possui um número de identificação (ID). Esse número, em hexadecimal, aparece depois do tamanho da chave. Exemplo: “pub 1024D/8C45C1CC 2006-10-26”. O número da chave é 8C45C1CC ou 8c45c1cc (não há distinção da caixa).

A criação e a manipulação das chaves

Criação das chaves

Para criar um par de chaves (pública e privada), utilize o comando:

ATENÇÃO: esta seção do artigo está desatualizada. O método de criação de chaves por *--gen-key* sem opções aditivas vai criar uma chave insegura, uma vez que o hash SHA-1 foi comprometido recentemente. Por enquanto, para criar chaves, siga o prescrito em http://it.slashdot.org/article.pl?sid=09/05/08/1429225 e http://wiki.softwarelivre.org/KSP/FISL10KSPNewKeyMiniHowto. Com isto, a minha nova chave é a c1cfc265. Em breve vou revogar a 8c45c1cc. (Observação incluída em 21 jul. 09)

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

Observações importantes:

- Ao criar as chaves, escolha a opção *DSA and Elgamal*. Essa opção irá permitir a assinatura e a criptografia de mensagens, arquivos etc.
- Opte pela não expiração das chaves para que ela seja "eterna". Chaves pessoais, geralmente, não são criadas com prazo de validade. No entanto, se preferir, insira uma data de expiração. Essa data poderá ser modificada de tempos em tempos na própria chave.
- O item *Comment* poderá ser deixado em branco mas, geralmente, é preenchido com um nickname que você use no mundo virtual.
- Não utilize acentos ao inserir o seu nome.
- Ao criar o par de chaves, será pedida uma passphrase (frase senha). Não utilize uma senha comum, com 6 ou 8 caracteres. Use uma frase retirada de uma música ou expressão que seja fácil de lembrar. A passphrase poderá ser alterada posteriormente.
- Ainda, em qualquer processo de criptografia assimétrica, a utilização da chave privada sempre irá requerer o uso de uma passphrase.

Listando as chaves existentes no chaveiro

Para listar as chaves, utilize o comando:

```
$ gpg --list-keys
```

Listando as assinaturas existentes em uma chave

Para listar as assinaturas existentes em uma chave, utilize o comando:

```
$ gpg --list-sigs <nr_da_chave>
```

Exemplo:

```
$ gpg --list-sigs 8C45C1CC
```

Exportando e importando chaves localmente

Os comandos a seguir serão utilizados apenas localmente. Para obter ou colocar chaves em servidores públicos na Internet, veja o item *Servidores públicos de chaves na Internet* (http://www.eriberto.pro.br/wiki/index.php?title=Usando_o_GnuPG#Servidores_p.C3.BAblicos_de_chaves_na_Internet).

Para exportar a sua chave pública como asc (para disponibilizar na Internet, por exemplo), utilize o comando:

```
$ gpg -a --export <nr_da_chave> > arq.asc
```

Para exportar a sua chave privada **(cuidado! perigo!)** como asc, utilize o comando:

```
$ gpg -a --export-secret-keys <nr_da_chave> > arq.key
```

Para importar uma chave para o seu chaveiro, utilize o comando:

```
$ gpg --import <arquivo_que_contém_a_chave>
```

Remoção de chaves do chaveiro

Para remover uma chave pública do chaveiro:

```
$ gpg --delete-keys <nr da chave>
```

Para remover uma chave privada do chaveiro:

```
$ gpg --delete-secret-keys <nr da chave>
```

Revogação de chaves

Para revogar uma chave:

```
$ gpg --gen-revoke <nr da chave> > <nr da chave>-revcert.asc
```

Para revogar uma chave será necessário saber a passphrase. Assim sendo, geralmente, logo após a geração do par de chaves, geramos também o certificado de revogação (para o caso de uso se houver a perda da senha). Guarde esse certificado em local seguro e sigiloso para evitar que alguma pessoa o utilize indevidamente.

Alteração da passphrase de uma chave

Para alterar a frase senha de uma chave, utilize o comando:

```
$ gpg --edit-key <nr da chave> password
```

password é uma palavra que faz parte do comando e não representa uma string a ser substituída pela senha a ser utilizada.

Para sair do ambiente de edição e salvar as alterações, digite “quit”.

Assinatura de uma chave pública alheia

Para assinar uma chave pública de outra pessoa, utilize o comando:

```
$ gpg --sign-key <nr da chave>
```

Caso você possua duas chaves e deseje especificar a chave que realizará a assinatura, utilize o comando:

```
$ gpg --sign-key <nr da chave>
```

Lembre-se de que o PGP (GPG) baseia-se em uma relação de confiança. Quanto mais assinaturas na sua chave, maior será o relação de confiança.

Listar assinaturas em chaves

Para listar as chaves, mostrando as assinaturas de cada chave, utilize o comando:

```
$ gpg --list-sigs
```

Listar os fingerprints em chaves

Para listar as impressões digitais de cada chave (fingerprint):

```
$ gpg --fingerprint
```

Adição e remoção de identidades (uid) nas chaves

Para adicionar uma nova identidade (nome e e-mail) a uma chave pré-existente, realize os seguintes procedimentos:

- Execute o comando *$ gpg --edit-key <nr_da_chave>*.
- No prompt de comando, digite *adduid* e pressione *ENTER*.
- Forneça as informações solicitadas.
- Saia do ambiente de edição com *quit*.

Para remover uma identidade extra inserida em uma chave, realize os seguintes procedimentos:

- Execute o comando *$ gpg --edit-key <nr_da_chave>*.
- No prompt de comando, digite *list* e pressione *ENTER*.
- Na frente de cada nome e e-mail será mostrado um número entre parênteses. Digite *uid nr*, onde *nr* deverá ser substituído pelo número que representa a identidade a ser eliminada. Pressione o *ENTER* para confirmar.
- Digite *deluid* e pressione o *ENTER* para eliminar a identidade.
- Saia do ambiente de edição com *quit*.

Determinando a identidade primária de uma chave

Caso você adicione identidades (uid) a uma chave, você poderá querer estabelecer qual delas será a primária. Para tanto:

- Execute o comando *$ gpg --edit-key <nr_da_chave>*.

- No prompt de comando, digite *list* e pressione *ENTER*.
- Na frente de cada nome e e-mail será mostrado um número entre parênteses. Digite *uid nr*, onde *nr* deverá ser substituído pelo número que representa a identidade a ser tornada primária. Pressione o *ENTER* para confirmar.
- Digite *primary* e pressione o *ENTER*. Será pedida a senha da atual identidade primária.
- Saia do ambiente de edição com *quit*.

A identidade primária sempre será a primeira exibida dentro do ambiente de edição. Imediatamente antes do nome completo do dono, será mostrado um caractere ponto.

Inserindo a sua foto na sua chave

A sua foto poderá ser inserida na sua chave. Isso, apesar de dispensável, ajudará na sua identificação. Siga os seguintes procedimentos:

- Crie uma foto JPG com até 288x240 pixels. Faça com que essa foto tenha, no máximo, 4 KB de tamanho. No meu caso, criei a foto em tons de cinza e com 155x140. No total, ela tem 2.4 KB. Veja a seguir:

O GPG só admite imagens JPG. Essa imagem não precisará estar com uma excepcional resolução.

- A seguir, edite a sua chave com o comando:

```
$ gpg --edit-key <ID_da_sua_chave>
```

- Digite *addphoto* e *ENTER*.
- Informe o nome da foto. Poderá aparecer a seguinte mensagem:

```
gpg: no photo viewer set
gpg: unable to display photo ID!
Is this photo correct (y/N/q)?
```

- Digite *y* e *ENTER* para responder a mensagem anterior. Será pedida a sua senha da chave privada.

Repare que a foto, na verdade, é uma nova ID dentro da chave. É como uma subchave.

- Digite *quit* e *ENTER* para sair.

Outras possibilidades

Para ver outras possibilidades de uso do comando *gpg*, utilize os comandos:

```
$ gpg --help
$ man gpg
```

Servidores de chaves públicas na Internet

Há vários servidores de chaves públicas na Internet. A maioria dos grandes servidores sincronizam chaves entre si. Cinco bons exemplos de servidores são:

- http://pgp.mit.edu
- http://pgp.surfnet.nl
- http://pgp.uni-mainz.de

Para ver a relação dos servidores existentes, consulte o endereço http://sks-keyservers.net/status.

Para ver uma das minhas chaves públicas, entre em qualquer um dos citados servidores e digite *eriberto* no campo de busca (Search String). Depois, clique em *Enviar dados*. Vão aparecer alguns "eriberto"s. Clique sobre 8C45C1CC e verá a chave. Para ver quem assinou esta chave, clique sobre o meu nome completo, na linha que contém 8C45C1CC (tela anterior, se você clicou na chave). Repare também que a chave possui mais de uma identidade. Ainda, observe o fingerprint. Repare que o fim do fingerprint sempre será igual ao número da chave (8C45C1CC).

Para encontrar outros servidores públicos, procure no Google por *pgp public servers*.

Para inserir uma chave em um servidor público, basta acessar o site do servidor (caso exista) e inserir a chave. Exemplo: http://pgp.mit.edu. Também é possível enviar a chave por intermédio de um comando. Exemplo:

```
$ gpg --keyserver subkeys.pgp.net --send-key <nr_da_chave>
```

Para buscar uma chave, utilize o comando:

```
$ gpg --keyserver <servidor> --recv-key <nr_da_chave>
```

Exemplo: para buscar a minha chave, utilize o comando:

```
$ gpg --keyserver subkeys.pgp.net --recv-key 8C45C1CC
```

É possível procurar chaves na Internet utilizando o Google. Exemplo de pesquisa: pgp pub fulano. Outra possibilidade é a de procurar por chaves dentro de um servidor, utilizando a sintaxe:

```
$ gpg --keyserver <servidor> --search-keys <nome ou e-mail ou domínio>
```

Exemplos:

```
$ gpg --keyserver subkeys.pgp.net --search-keys Eriberto
$ gpg --keyserver subkeys.pgp.net --search-keys eriberto.pro.br
```

Imediatamente após a pesquisa, será possível incluir um dos resultados no chaveiro.

Caso haja a necessidade de revogar um par de chaves, envie o certificado de revogação para o servidor público. Um par de chaves inserido em um servidor público não pode ser apagado; somente poderá ser revogado.

Há ainda uma outra possibilidade interessante: a de atualizar todas as chaves do seu chaveiro a partir de um servidor na Internet. Um exemplo:

```
gpg --refresh-keys --keyserver keyserver.noreply.org
```

Relação de confiança

O uso do PGP baseia-se em uma relação de confiança. Assim sendo, geralmente, uma chave pública deverá ser assinada pela chave privada de várias pessoas conhecidas. Esse processo deverá ser presencial, para garantir que não haja quebra da cadeia de confiança. Um exemplo clássico: uma pessoa envia a sua chave, por e-mail, para que outra assine. Como garantir que o receptor terá a certeza de que o emissor seja realmente a pessoa que ela diz ser?

Mais adiante será mostrado, de forma mais ampla e detalhada, o processo de assinatura de chaves.

Armazenamento em CD Card, Pen Drive e Smart Card

Geralmente, armazenamos o par de chaves e o respectivo certificado de revogação em pendrives, smart cards ou em um CD Card. O CD Card tem o tamanho de um cartão de crédito, uma capacidade de 50 MB de dados. A foto a seguir mostra um CD Card: As principais vantagens do CD Card são o baixo custo, o pequeno volume e a confiabilidade. Também poderá ser utilizado um smartcard (exatamente igual a um cartão de banco). Para isso, será necessária a utilização de uma gravadora de cartão. Os usuários necessitarão de leitoras de cartão. A pendrive será útil para que outras pessoas possam assinar a sua chave.

O processo para a assinatura de chaves de pessoas conhecidas

Cuidados fundamentais

Chaves alheias somente deverão ser assinadas se executados os seguintes procedimentos:

- Faça um **contato físico** com a pessoa cuja respectiva chave você irá assinar. **Repito: você deverá estar frente a frente com a pessoa.**
- Obtenha dessa pessoa os seguintes dados:
  - Nome completo, como consta na chave;
  - Endereço de e-mail, como consta na chave;
  - O fingerprint da chave a ser assinada.
- Ainda, confira a identidade da passoa, **mesmo que a conheça há muito tempo**, por intermédio de um documento com foto. Verifique se o nome completo é idêntico ao fornecido. Geralmente, utilizamos carteira de identidade ou de motorista.

ATENÇÃO: não negligencie os passos mostrados neste item. Eles irão garantir que a pessoa é quem realmente diz ser e que o fingerprint apresentado realmente pertence a ela. **Não assine** chaves tendo

como base uma mensagem de e-mail, conversas telefônicas, contato por MSN etc. Se você fizer isso, poderá comprometer seriamente a cadeia de confiança. ***Em assuntos que envolvem segurança, todo o cuidado é pouco!***

O uso do cartão de visita

É muito comum as pessoas confeccionarem cartões de visita já contendo o fingerprint. Isso facilita bastante o contato pessoal, pois evita a necessidade de anotar os dados no momento do encontro (acredite, isso dá trabalho). A seguir, um exemplo de cartão de visita com os dados básicos (além de outros):

Note que o cartão mostrado não difere de um cartão de visita comum, do tipo que você entregaria a qualquer pessoa. O único dado extra é o fingerprint. Ainda, o telefone celular foi desfigurado, pois este realmente é o meu cartão.

Lembre-se! São dados essenciais num cartão usado para assinar chaves PGP: o nome completo, o e-mail e o fingerprint da chave. Esses dados deverão ser verificados em um documento oficial que contenha foto.

Você não precisa usar exatamente um cartão, apesar de ser elegante. A idéia é facilitar as coisas na hora de trocar dados com outras pessoas. Então, você pode imprimir seus dados (em forma de tabela) em uma folha de papel e recortar os quadrados. Veja um exemplo disso a seguir:

João Eriberto Mota Filho eriberto@eriberto.pro.br **1024D/8C45C1CC:** 3BBA FF35 8B92 039F FC0B 673F 5088 841B 8C45 C1CC	João Eriberto Mota Filho eriberto@eriberto.pro.br **1024D/8C45C1CC:** 3BBA FF35 8B92 039F FC0B 673F 5088 841B 8C45 C1CC	João Eriberto Mota Filho eriberto@eriberto.pro.br **1024D/8C45C1CC:** 3BBA FF35 8B92 039F FC0B 673F 5088 841B 8C45 C1CC
João Eriberto Mota Filho eriberto@eriberto.pro.br **1024D/8C45C1CC:** 3BBA FF35 8B92 039F FC0B 673F 5088 841B 8C45 C1CC	João Eriberto Mota Filho eriberto@eriberto.pro.br **1024D/8C45C1CC:** 3BBA FF35 8B92 039F FC0B 673F 5088 841B 8C45 C1CC	João Eriberto Mota Filho eriberto@eriberto.pro.br **1024D/8C45C1CC:** 3BBA FF35 8B92 039F FC0B 673F 5088 841B 8C45 C1CC
João Eriberto Mota Filho eriberto@eriberto.pro.br	João Eriberto Mota Filho eriberto@eriberto.pro.br	João Eriberto Mota Filho eriberto@eriberto.pro.br

Execução da assinatura

De posse dos dados da pessoa que deseja a sua assinatura na chave pública dela, você deverá seguir alguns procedimentos para executar tal assinatura. A partir deste momento, toda a sua atenção deverá estar voltada para constante verificação da veracidade dos dados a serem manipulados.

Inicialmente, busque, em um servidor público, a chave pública a ser assinada:

```
$ gpg --keyserver subkeys.pgp.net --recv-key <ID_da_chave_a_ser_assinada>
```

A chave poderá ser adquirida a partir de um disquete, CD ou pendrive. No entanto, este método é menos usual, uma vez que espera-se que a mesma esteja disponível para o mundo em um servidor na Internet.

A seguir, liste alguns dados da chave com o comando:

```
$ gpg --fingerprint <ID_da_chave_a_ser_assinada>
```

Confira atentamente o ID da chave, o fingerprint, o nome completo e o e-mail que forem mostrados. Uma vez conferidos os dados, assine a chave com o comando:

```
$ gpg --sign-key <ID_da_chave_a_ser_assinada>
```

ATENÇÃO: Nunca assine uma chave se não tiver adotado os **cuidados fundamentais** para realizar tal assinatura!

Caso você tenha mais de uma chave e deseje escolher a chave que fará a assinatura, utilize a opção *-u*. Exemplo:

```
$ gpg -u <ID_da_chave_que_realizará_a_assinatura> --sign-key <ID_da_chave_a_ser_assinada>
```

Envio da chave assinada para o seu dono

Depois de assinada a chave, exporte-a em formato ASCII:

```
$ gpg -a --export <ID_da_chave_assinada> > nome.asc
```

Comprima a chave com GZIP para evitar que, no envio, a chave, por estar em ASCII, deixe de ser anexo e vire parte do texto:

```
$ gzip nome.asc
```

Envie, por e-mail, o arquivo *.gz* para o dono da chave.

Inserindo a chave assinada no chaveiro e no servidor público

Ao receber a chave assinada, o dono da mesma deverá importá-la e, a seguir, fazer upload para o servidor público. Essas ações irão forçar uma atualização de tal chave no chaveiro e no servidor.

Caso você seja o dono da chave e esteja recebendo-a, para importá-la, utilize o comando convencional:

```
$ gpg --import <arquivo_que_contém_a_chave>
```

Para enviar a chave assinada para o servidor, também utilize o comando convencional para esse tipo de ação:

```
$ gpg --keyserver subkeys.pgp.net --send-key <nr_da_chave>
```

Um fato interessante: você mesmo poderá atualizar uma chave alheia em um servidor público depois de assiná-la, utilizando o comando anterior. No entanto, é melhor enviar para o dono da chave para que ele mesmo faça isso, uma vez que ele poderá querer utilizar um servidor público específico.

Determinando a confiabilidade das chaves alheias

Após importar uma ou mais chaves para o seu chaveiro, você poderá, se quiser, determinar o grau de confiabilidade que você terá no dono delas, em relação a outras chaves. Exemplo: você pode dizer que confia plenamente nas chaves que Ana assina. Assim, quando você receber a chave de Beto, que foi assinada por Ana, terá motivos para confiar nessa chave, mesmo não conhecendo Beto. Algumas considerações importantes:

- Não é aconselhável confiar em uma chave alheia só porque determinada pessoa a assinou. Essa confiança ocorre, geralmente, em casos de emergência.
- É possível utilizar esse artifício com pessoas extremamente sérias e responsáveis, diminuindo o tamanho do seu chaveiro.

Existem o seguintes níveis de confiabilidade:

- **Unknown**: Não se sabe como a pessoa em questão procede ao assinar uma chave. Ainda não se pode observar a seriedade e responsabilidade dessa pessoa ao assinar chaves. Não se deve confiar nas assinaturas dessa pessoa em chaves alheias.
- **None**: Esta pessoa costuma assinar chaves **sem** certificar-se de que elas realmente são da pessoa que diz possuí-las. Não se deve confiar nas assinaturas dessa pessoa em chaves alheias.
- **Marginal**: Esta pessoa assina chaves de forma correta (faz as verificações físicas necessárias). É possível confiar nessa pessoa, **caso seja extremamente necessário**.
- **Full**: O usuário conhece muito bem sistemas criptográficos, é extremamente confiável e responsável. Qualquer chave assinada por esse usuário será extremamente confiável. É possível pensar em aceitar algo de outras chaves que tenham sido assinadas por essa pessoa.

Para determinara a confiabilidade de cada chave, execute o comando:

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

Com isso, serão apresentadas as chaves, uma por uma, e você deverá selecionar uma das seguintes opções:

```
1 = I don't know or won't say  (= unknown)
2 = I do NOT trust             (= none)
3 = I trust marginally         (= marginal)
4 = I trust fully              (= full)
```

s = skip this key	(ignore esta chave)
q = quit	(saia e volte para o prompt, ignorando as demais chaves)

Uso do GnuPG para assinar e criptografar mensagens de e-mail

Os clientes de e-mail podem utilizar o GPG para assinar/criptografar mensagens. Para isso, existem alguns plugins.

Mozilla Thunderbird (ou Icedove) e o GnuPG

O Enigmail permite o uso do GnuPG no Mozilla Thunderbird, atual Icedove no Debian.

Para instalar o Enigmail no Debian, utilize o comando:

```
# apt-get install enigmail enigmail-locale-pt-br
```

O site do Enigmail é http://enigmail.mozdev.org.

MS Outlook Express e o GnuPG

O GPGOE permite o uso do GnuPG no Outlook Express. O site para download e documentação é http://winpt.cityofcambridge.net/gpgoe.html.

GMail, Mozilla Firefox (ou Iceweasel), FireGPG e o GnuPG

Isso mesmo! Há como usar o GnuPG no GMail ou em outro webmail qualquer, caso você esteja usando o Mozilla Firefox, atual Iceweasel no Debian. Basta utilizar a extensão FireGPG, que pode ser encontrada em http://firegpg.tuxfamily.org.

Assinando e criptografando arquivos

Ex: envio de uma topologia pelo google ou de um código para um amigo.

```
$ gpg -a --sign <arquivo>
```

ou

```
$ gpg --clearsign <arquivo>
```

Frontends gráficos

kgpg seahorse

Outros não testados: http://www.gnupg.org/(en)/related_software/frontends.html#gui.

Ferramentas especiais no Debian GNU/Linux

signing-party gpg-key2ps

Ferramentas para MS Windows

Ver http://www.gpg4win.org

Veja também

- Como preparar-se para uma festa de assinatura de chaves GPG

Links externos

- Debian: assinatura de chaves (http://www.debian.org/events/keysigning.pt.html)
- Public key fingerprint (http://en.wikipedia.org/wiki/Public_key_fingerprint)

Comentários, sugestões e controle de acessos

Por favor, **deixe os seus comentários e sugestões sobre este artigo** no meu Blog Técnico. Para isto, clique aqui (http://www.eriberto.pro.br/blog/?p=535).

Consulte também o contador abaixo, iniciado em 15 abr. 07, além do gráfico acima.

Disponível em "http://eriberto.pro.br/wiki/index.php?title=Usando_o_GnuPG&oldid=1517"

- Esta página foi modificada pela última vez em 16 de novembro de 2011, às 11h37min
- Conteúdo disponível sob Creative Commons - Atribuição - Uso Não Comercial - Partilha nos Mesmos Termos, salvo indicação em contrário.