


Gnu Privacy Guard

GnuPG

(Mini Howto – Português–Brasil)

 Erro de leitura

Tradução: Renato Martini
rmartini@cipsga.org.br

Junho de 2000

Gnu Privacy Guard

GnuPG

(Mini Howto – Português–Brasil)

Comite de Incentivo a Produção
do Software Gratuito e Alternativo
CIPSGA

Tradu;a'o:

Renato Martini
rmartini@cipsga.org.br

Junho de 2000

Arte Final:

Djalma Valois Filho
dvalois@cxpostal.com

Copyright (c) 2000, Renato Martini.

Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.1 or any later version published by the Free Software Foundation; with the Invariant Sections being LIST THEIR TITLES, with the Front-Cover Texts being LIST, and with the Back-Cover Texts being LIST.

A copy of the license is included in the section entitled "GNU Free Documentation License".

Copyright (c) 2000, Renato Martini

E garantida a permissão para copiar, distribuir e/ou modificar este documento sob os termos da GNU Free Documentation License, versão 1.1 ou qualquer outra versão posterior publicada pela Free Software Foundation; sem obrigatoriedade de Seções Invariantes na abertura e ao final dos textos.

Uma copia da licença deve ser incluída na seção intitulada GNU Free Documentation License.

Gnu Privacy Guard

GnuPG

Mini Howto

(Português–Brasil)

Renato Martini (português–Brasil) <rmartini@cipsga.org.br>

Dindart Jean–François (francês) <dindart@labri.u-bordeaux.fr>

Brenno J.S.A.A.F.de Winter (inglês) <brenno@dewinter.com>

Michel Fisher v. Mollard (alemão) <fischer@math.uni-goettingen.de>

Versão 0.1.0 de 10 de outubro de 1999 (francesa)

Versão 0.1 de 18 de junho de 2000 (brasileira)

Este mini HOWTO apresenta as bases para a utilização do GNU Privacy Guard

(GnuPG), uma implementação Open Source do OpenPGP. Para permanecer livre de toda licença de utilização, esta implementação não utiliza nem o algoritmo RSA, nem qualquer algoritmo patenteado. A versão original deste documento

Foi escrita em alemão por Michael Fischer v. Mollard. Esta versão em português é baseada na tradução francesa, e cotejada com a versão inglesa do documento.

Índice geral

PREAMBULO	5
1. ALGUNS DADOS SOBRE CRIPTOSISTEMAS	6
1.1 <i>O que é um criptosistema?</i>	6
1.2 <i>O que é um criptosistema de chave pública?</i>	6
1.3 <i>O que é uma assinatura digital?</i>	7
1.4 <i>Porque assinar uma chave pública?</i>	7
1.5 <i>O que é um certificado de revogação?</i>	8
1.6 <i>É possível ler minhas mensagens criptografadas sem meu acordo quando uso o GnuPG?</i>	8
2. INSTALAÇÃO DO GnuPG	9
2.1 <i>Onde pegar as fontes do GnuPG?</i>	9
2.2 <i>Como configurar a compilação do GnuPG?</i>	10
2.3 <i>Como compilar o GnuPG?</i>	11
2.4 <i>Como instalar o GnuPG?</i>	11
3. O GERENCIAMENTO DAS CHAVES	12
3.1 <i>Como gerar o par 'chave pública/chave privada'?</i>	12
3.2 <i>Como tornar pública a sua chave pública?</i>	14
3.3 <i>Como acrescentar uma chave pública ao seu chaveiro digital?</i>	15
3.4 <i>Como publicar o conteúdo do seu chaveiro digital?</i>	15
3.6 <i>Como publicar a 'impressão digital' (fingerprint) de uma chave pública de seu chaveiro digital?</i>	16
3.7 <i>Como assinar uma chave pública de seu chaveiro digital?</i>	16
3.8 <i>Como gerar um certificado de revogação para um de seus pares de chaves?</i>	17
3.9 <i>Como modificar uma chave pública do seu chaveiro digital?</i>	17
4. CRIPTOGRAFIAR E DESCRIPTOGRAFIAR	17
4.1 <i>Como criptografar uma mensagem?</i>	18
4.2 <i>Como descriptografar uma mensagem?</i>	18
5. ASSINAR E VERIFICAR ASSINATURAS	19
5.1 <i>Como assinar uma mensagem?</i>	19
5.2 <i>Como verificar a assinatura de uma mensagem?</i>	20
6. DOCUMENTAÇÕES SUPLEMENTARES	20
6.1 <i>GnuPG</i>	20
6.2 <i>PGP20</i>	
6.3 <i>Servidores de chaves</i>	21
6.4 <i>Livros</i>	21
7. VERSÕES DESTE DOCUMENTO	21
7.1 <i>Esclarecimentos sobre a versão inglesa</i>	21
7.2 <i>Esclarecimentos sobre a versão francesa</i>	22
7.3 <i>Esclarecimentos sobre a versão brasileira</i>	22
CONTROLE DA VERSÃO EM PORTUGUÊS	24
GNU FREE DOCUMENTATION LICENSE.....	25

Preambulo

Copyright (c)2000 Renato Martini (versão portuguesa–Brasil)

Copyright (c)1999 Dindart Jean–François (versão francesa)

Copyright (c)1999 Brenno J.S.A.A.F. de Winter (versão inglesa)

Copyright (c)1999 Michael Fischer v. Mollard (versão alemã original)

Este documento é uma distribuição que pode ser livremente redistribuída e/ou modificada segundo os termos da GNU Library General Public License publicada pela Free Software Foundation, versão 2 ou superior.

Este documento é redistribuído na esperança que seja útil, mas sem NENHUMA GARANTIA quanto a sua correção. Para obter mais detalhes quanto a estes termos consulte a GNU Library General Public License.

Você pode obter uma cópia da GNU Library License escrevendo para a Free Software Foundation, Inc., 59 temple Place – Suite 330, Boston, MA 02111–1307, USA.

No Brasil você pode contactar o Comitê de Incentivo à Produção do Software Gratuito e Alternativo (CIPSGA), <http://www.cipsga.org.br>, ou enviando um e-mail para licenca@cipsga.org.br.

1. Alguns dados sobre criptosistemas

1.1 O que é um criptosistema?

As missões essenciais de um criptosistema podem ser resumidas em três:

- * Integridade: a mensagem recebida é indistinguível da mensagem enviada,
- * Confidencialidade: a mensagem é incompreensível a toda pessoa não autorizada,
- * Autenticação: a autenticidade da mensagem é verificável.

Portanto, pode-se definir um criptosistema como um sistema que assegura a confidencialidade, a integridade e a autenticação de mensagens que passam em canais de comunicações. Para certas utilizações, como o estabelecimento de contratos ou provas, um criptosistema pode também assegurar o não repúdio de mensagens, isto é, assegurar que seja impossível a qualquer um repudiar uma de suas mensagens.

1.2 O que é um criptosistema de chave pública?

Até 1976, os criptosistemas baseavam-se em somente uma chave. Essa chave é utilizada ao mesmo tempo para criptografar e descriptografar, de maneira que qualquer um que possua essa chave é capaz de ler e escrever qualquer mensagem criptografada com essa chave. Tais criptosistemas possuem de fato duas pressuposições para sua utilização:

1. o remetente e o destinatário devem trocar a chave criptográfica antes de poder trocar mensagens criptografadas.
2. a troca da chave necessita da existência de um canal de transmissão protegido de toda escuta exterior para evitar que um intruso possa conhecer a chave para criptografar.

Estas duas pressuposições sendo muito difíceis a serem satisfeitas na maior parte dos casos, Whitfield DIFFIE e Martin HELLMAN propõem em 1976 um novo princípio de criptosistema: a criptografia de chave pública. Os criptosistemas desse tipo utilizam duas chaves com papéis bem distintos. A primeira chave é chamada 'chave pública' já que ela é conhecida por todos. É a chave pública do destinatário de uma mensagem que é usada para criptografar uma mensagem. A segunda chave, chamada 'chave privada', é conhecida

somente por seu proprietário e serve para descriptografar as mensagens criptografadas com sua chave pública. O caráter público da primeira chave permite a troca de mensagens entre duas pessoas sem comunicação direta prévia entre duas partes, nem canal de transmissão protegido.

Se a chave privada vier a ser descoberta por um intruso, o segredo das mensagens criptografadas com essa chave privada e a chave pública correspondente é comprometido. Portanto, o maior cuidado deve ser contribuir para a preservação do segredo da chave privada. Em particular, essa chave JAMAIS deve ser comunicada através de um canal que não seja absolutamente seguro. Uma consequência é que, sobre um plano prático, a utilização do GnuPG através de uma conexão de rede deve ser excluída, por mais que esta rede seja acessível somente a poucas pessoas exteriores. É evidente então que a segurança é uma cadeia cujo o nível é igual àquele de seu nó mais fraco.

1.3 O que é uma assinatura digital?

Contrariamente ao que seu nome nos faz pensar, uma assinatura digital é muito mais do que o similar digital da assinatura manuscrita. Por certo, a assinatura digital é função do remetente e do conteúdo da mensagem. Portanto, uma assinatura testemunha simultaneamente a autenticidade da origem suposta e a integridade de uma mensagem. Por exemplo, a utilização sistemática de assinaturas em arquivos instalados em seu sistema reduz consideravelmente os ricos de 'Trojan Horses'.

Tecnicamente falando, uma assinatura digital é apenas uma chave de corte calculado sobre toda a mensagem e que é criptografada com a chave secreta do remetente. Verificar a assinatura de uma mensagem, por conseguinte, ocorre simplesmente ao se recalcular a chave a partir do texto descriptografado e em compará-la com a assinatura descriptografada com a ajuda da chave pública do suposto remetente. Se as duas chaves são idênticas, a assinatura é dita válida, ou seja, que pode-se razoavelmente pensar que o remetente da mensagem é aquele que pretende sê-lo e que a mensagem não foi modificada no curso da transmissão.

1.4 Porque assinar uma chave pública?

O calcanhar de Aquiles dos criptosistemas de chave pública reside na distribuição das chaves públicas. Por certo, se um intruso consegue fazer com que você aceite sua chave pública como a chave pública de um de seus interlocutores, ele poderá ler todas as suas mensagens e mesmo respondê-las fazendo-se passar por seu interlocutor! Se ele envia suas mensagens ao seu interlocutor utilizando-se da verdadeira chave pública de seu interlocutor, será cada vez mais difícil descobrir que um intruso leu todas as suas mensagens.

A solução adotada pelo PGP, e portanto pelo GnuPG, consiste em assinar às chaves públicas. A idéia é que se você dispõe de uma chave pública na qual tem toda a confiança, então pode estender sua confiança em todas as chaves públicas assinadas por tal chave, certamente, após ter verificado a assinatura. Uma vez que você põe toda a confiança nessas novas chaves, você pode servir-se delas para verificar outras chaves, e por aí adiante. O problema se reduz agora a como ter confiança nesta primeira chave. A solução consiste em dispor de um canal de comunicação que assegure a integridade e a autenticação das mensagens para comparar a 'impressão digital' de uma chave pública que você recebeu com a 'impressão digital' calculada pelo proprietário da chave pública. Este canal pode, por exemplo, ser o telefone ou um encontro direto.

O GnuPG permite modificar o nível de confiança, variando de 1 ('eu não sei') a 4 ('confiança total'), de cada uma das chaves públicas que você possua. O GnuPG sabe igualmente calcular de forma automática o nível de confiança de uma chave em função dos níveis de confiança das assinaturas desta chave. Portanto, você deve somente pôr sua confiança com o maior cuidado se você não deseja comprometer a segurança de seu criptosistema e dos criptosistemas de todos aqueles que confiam em você!

1.5 O que é um certificado de revogação?

Quando não convém mais, seja porque a chave privada foi descoberta ou porque o tamanho da chave se mostrou muito pequeno ou por qualquer outra razão, você pode revogar tal par de chaves. Um certificado de revogação faz saber publicamente que você não usa mais um de seus pares de chaves. Para evitar que qualquer um possa gerar tal certificado, este é assinado pelo chave privado do par a ser revogado. A validade de um certificado de revogação é assim comodamente verificável por todos.

1.6 É possível ler minhas mensagens criptografadas sem meu acordo quando uso o GnuPG?

É evidente que a confidencialidade das mensagens que você troca usando GnuPG não depende somente da qualidade do GnuPG ou de seus algoritmos escolhidos, mesmo se esse último tem muita influência nisto. A valoração do nível de confidencialidade de suas mensagens deve levar em conta o conjunto de seu sistema. O nível de confidencialidade do PGP parece inteiramente razoável já que nenhuma história de ataque ao PGP foi até agora relatada. Certamente, se uma entidade qualquer tiver êxito em quebrar o PGP, é pouco provável que ela o anuncie publicamente, porém numerosos experts estudaram atentamente os algoritmos usados sem neles descobrir falhas. No entanto, mesmo se o PGP parece razoavelmente seguro, permanecem numerosas vias de ataque, principalmente pelo viés de seu sistema operacional, por exemplo nele instalando sem o seu conhecimento um programa com a tarefa de analisar tudo o que o usuário digita no teclado a procura de senhas, para então enviá-las pela rede para um endereço preciso! Se você acha que se trata de ficção, pense na facilidade com a qual os vírus se instalam em

certos sistemas operacionais. Estes sistemas operacionais, mesmo os mais recentes, são particularmente sensíveis a esse tipo de ataque e devem desde então excluir a possibilidade de que o nível dos intrusos potenciais ultrapasse o de um iniciante em informática. Por certo, é inútil usar um criptosistema que exige um cálculo gigantesco para quebrar uma mensagem se seu sistema operacional é uma verdadeira peneira! Entretanto, seu sistema operacional não é o único ângulo de ataque, uma senha simples para a adivinhação, uma pessoa ingênua em seu escritório, a aceitação de uma chave pública sem a devida verificação, etc., são alguns dos meios que permitem o comprometimento da confidencialidade de suas correspondências, e sem falar de meios mais custosos e mais sofisticados.

Estas observações não desejam tornar a ninguém paranóico, mas sim tomar consciência que a segurança é um todo. A criptografia não é a panaceia neste domínio. É necessário também que você compreenda que a confidencialidade absoluta é irrealizável (salvo se você não precisa mais recuperar o conteúdo de uma mensagem, uma vez que ela foi criptografada), mas provavelmente você não tem necessidade de tal confidencialidade. O ideal é adaptar seus meios à ameaça.

2. Instalação do GnuPG

2.1 Onde pegar as fontes do GnuPG?

O software GnuPG é disponível em diversos sites, mas o melhor para o download é o seu sítio oficial. Você também encontrará aí os endereços de espelhamento (mirrors). Se já dispõe de uma versão instalada do GnuPG ou do PGP, é bastante recomendado tirar vantagem disso e verificar as fontes do GnuPG que você pegou, para verificar enfim se elas são as autênticas.

O software GnuPG está disponível como pacotes Debian ou Red Hat, e como fontes. Os pacotes Debian e Red Hat se instalam diretamente com a ajuda de ferramentas de instalação fornecidas com as distribuições correspondentes e sua instalação não é abordada neste documento. Os passos a seguir, para instalar o GnuPG a partir das fontes, é detalhado logo abaixo. Se você instalar o GnuPG numa arquitetura ou num sistema diferente dos inicialmente previstos, seria bom que chegasse aos autores do GnuPG os detalhes da sua instalação, que poderão beneficiar assim muitos outros usuários. A lista dos sistemas operacionais nos quais o GnuPG foi compilado com sucesso está disponível no sítio oficial do GnuPG.

NOTA: A regulamentação dos EUA restringe muito severamente a exportação de produtos com criptografia forte.

Essa regulamentação tem duas consequências importantes. A primeira é que é ilegal fazer o download do GnuPG num sitio hospedado no território norte-americano, a partir de um computador fora dos EUA. A segunda é que existe uma versão internacional e uma versão nacional (destinada aos EUA) do software PGP, é interessante notar também que você é livre para o download da versão internacional do PGP a partir de uma máquina situada no território dos EUA, mas você estará todavia totalmente proibido de deixar este país com tal versão!

ANEDOTA: As fontes da versão internacional foram legalmente exportadas sob a forma de um livro que foi em seguida digitalizado em Oslo. Você encontrará outras informações sobre o tema no sitio 'International PGP Homepage'.

2.2 Como configurar a compilação do GnuPG?

Descompactar as fontes do GnuPG:

```
tar xvf gnupg-?.?.?.tar.gz
```

depois vá para o diretório criado pelo comando precedente e execute a configuração das fontes do GnuPG para o seu sistema:

```
./configure
```

Por padrão, o GnuPG se instala nos diretórios onde somente o root pode escrever. Se você não tem os privilegios de super-usuário, você pode mudar o diretório básico dos diretórios de instalação:

```
./configure --prefix=OutroDiretório
```

Nesse caso, você precisará também acrescentar o diretório 'OutroDiretório/bin' a sua variável de ambiente PATH.

Se nenhuma mensagem de erro aparece no final da configuração, é que ela ocorreu sem problemas. No caso de um problema com a internacionalização (gettext) do GnuPG, você pode tentar:

```
./configure --with-included-gettext  
ou
```

```
./configure --disable-NLS
```

Se uma mensagem de erro aparece ao longo desta configuração, você pode consultar o arquivo 'config.log' que contém todos os detalhes a respeito do desdobramento do processo de configuração.

A configuração das fontes é um processo cheio de parâmetros. Você pode ver todas as opções de configuração possíveis usando a opção '--help':

```
./configure --help
```

2.3 Como compilar o GnuPG?

Para efetuar a compilação, basta agora digitar:

```
make
```

A compilação deve acontecer sem problemas. Se houver algum, você deve consultar o arquivo "BUGS" fornecido com as fontes do GnuPG. Se esse arquivo não for suficiente, pode pedir ajuda postando suas questões (seja PRECISO) na lista de discussão adequada do GnuPG.

2.4 Como instalar o GnuPG?

A instalação usa o mesmo comando que a compilação mas com a opção 'install':

```
make install
```

Lembre que por padrão a instalação acontecerá nos diretórios acessíveis unicamente com os privilégios de super-usuário. Se você não os têm, deve-se modificar os diretórios de instalação no momento da configuração como vimos acima.

Se você tem os direitos de usuário root, pode decidir alterar o 'suid bit' do executável gpg. O interesse é que assim, o gpg poderá impedir o sistema de partilhar dados confidenciais com o disco rígido. O inconveniente é que se você não pôde verificar a autenticidade das fontes do GnuPG trazidas por download. Existe então uma probabilidade que não deve ser desconsiderada que tais fontes tenham sido modificadas de forma mal intencionada (Trojan

Horse). Nesse caso, dar direitos de execução root a tal programa compromete fortemente a segurança do seu sistema, se esse não é o seu funcionamento correto. Para ser completo, mesmo no caso em que você verificou a autenticidade das fontes do GnuPG, é necessário ainda interrogar à autenticidade da assinatura do qual você se serviu, do programa utilizado para recuperar esta assinatura, do programa utilizado para verificar a assinatura das fontes, etc. A atribuição dos direitos de execução root ao gpg não é portanto uma decisão tranquila.

Se você escolhe não pôr os direitos de execução root ao gpg ou que você não tenha privilégios de root, o gpg mostrará uma mensagem de advertência cada vez que dados confidenciais correm o risco de serem escritos no disco rígido após um swap:

Warning: using insecure memory!

Você pode desativar o aparecimento da mensagem de advertência acrescentando a opção 'no-secmem-warning' no seu arquivo '~/.gnupg/options'.

3. O gerenciamento das chaves

Uma vez instalado o GnuPG, você pode começar a utilizá-lo para proteger o conteúdo de suas mensagens de olhares indiscretos. O envio de uma mensagem apela à sua chave privada para a operação de assinatura e à chave pública do destinatário para a operação de criptografia. O número de chaves em sua posse está portanto diretamente ligado ao número dos seus interlocutores, sem contar que você pode escolher ter vários pares de chave privada/chave pública. O conjunto dessas chaves é chamado de um chaveiro digital e o GnuPG fornece os comandos para geri-lo.

3.1 Como gerar o par 'chave pública/chave privada'?

A primeira operação a realizar é a geração de um par chave privada/chave pública com o comando '--gen-key':

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

Este comando gera um novo par de chaves, uma privada e uma pública baseando-se em suas respostas a algumas questões. A primeira diz respeito ao algoritmo criptográfico e de assinatura que você deseja usar. Você encontrará informações sobre os algoritmos propostos no PGP DH versus RSA FAQ e sobretudo na excelente obra de Bruce Schneier: Criptografia Aplicada. A escolha DSA e ElGamal deve ser privilegiada, visto a sua utilização

na Internet. Se você escolhe somente utilizar o algoritmo ElGamal, será pedida a sua confirmação para essa escolha (as implicações serão precisadas).

A segunda questão diz respeito ao tamanho de sua chave criptográfica ou de assinatura se escolheu gerar uma chave de assinatura somente. A resposta a esta questão depende enormemente do uso que intenta fazer. Para o algoritmo DSA, o tamanho da chave é geralmente de 1024 bits. Para ElGamal, você poderá escolher um tamanho entre 768 bits e 2048 bits. De forma absoluta: quanto maior é uma chave melhor. No entanto, o tempo de criptografia aumenta com o tamanho de sua chave. Se você não tem idéia precisa quanto ao tamanho necessário, o melhor é escolher o tamanho proposto como padrão. Se o uso deste tamanho se mostra inadequado, você sempre poderá gerar um novo par de chaves mais adaptados as suas necessidades.

As questões seguintes servem para coleta de informação que servirá mais tarde para distinguir sem ambiguidade esse novo par de chaves entre todos os pares de chaves que você possui. É graças a essas informações, por exemplo, que você poderá escolher o par de chaves para utilizar para assinar uma mensagem. Por conseguinte, você deve entrar com um nome, um endereço de e-mail e um comentário. O comentário sendo um campo livre é muito prático para distinguir seus pares de chaves uns dos outros. Todas essas informações e um gerador de números pseudo-aleatórios serão em seguida usados para gerar um novo par de chaves. Você posteriormente poderá modificar, se desejar, as informações contidas num par de chaves.

Somente resta escolher uma frase-chave que servirá para criptografar sua chave privada para poder estocá-la sem riscos no seu disco rígido. Esta frase será pedida cada vez que você quiser utilizar sua chave privada. Dito de outra forma: se você esquecer a frase-chave de um par de chaves, você não poderá mais utilizá-lo! Portanto, você deve se precaver contra esse tipo de risco sem pôr em perigo a confidencialidade de sua frase-chave. Por certo, a segurança de suas mensagens repousa na confidencialidade de sua chave privada e a confidencialidade de sua chave privada e também da sua frase-chave. Portanto, a primeira medida a ser tomada é escolher uma frase-chave robusta. O problema aqui é que não existe uma definição rigorosa de 'robusto'. Podemos somente dar alguns conselhos:

- * a frase-chave deve ser longa,
- * a frase-chave deve conter caracteres alfabéticos, pontuação, algarismos, caracteres especiais,
- * a frase-chave não deve EM NENHUM CASO ser uma data de nascimento, um nome, um numero de documento pessoal, uma palavra ou algo fácil de se adivinhar, nem mesmo uma concatenação de dados desse tipo.

A escolha de uma boa frase-chave é difícil, mas não esqueça que uma cadeia jamais é mais sólida que a sua malha mais fraca. VoCê POdE MelhORaR A SeGURanÇA de sUa FrAsE-CHaVe USANDO maiúscuLAS e MINúsculaS (mas não somente!) dE FORMa iRreGuLAR.

A segunda medida consiste em gerar um certificado de revogação para todo novo par de chaves. O motivo de se proceder assim é que é necessário dispor da chave privada, e portanto da frase-chave, para gerar o certificado de revogação de um par de chaves. gerar um certificado de revogação o mais cedo possível irá proteger do esquecimento da sua chave. Certamente, você deverá também conservar esse certificado protegido.

Um vez que todas as informações foram dadas, o cálculo da chave começa. O gerador de números pseudo-aleatórios necessita de um grande número de dados aleatórios, o que é difícil num computador. Você pode melhorar a qualidade dos resultados do gerador de números pseudo-aleatórios gerando você mesmo um pouco de acaso, por exemplo, mexendo o seu mouse, digitando no seu teclado, executando aplicativos, etc. A utilização de pseudo-acaso é necessária para assegurar que não é possível obter a sua chave privada efetuando o mesmo cálculo que o seu. Na verdade, as chances de sucesso de tal ataque estão diretamente ligadas à qualidade do pseudo-acaso gerado pelo gerador de números pseudo-aleatórios.

3.2 Como tornar pública a sua chave pública?

Seus pares de chaves são estocados no seu sistema e o comando '—export' permite a extração da chave pública de um par de chaves e de escrevê-lo na saída padrão:

```
gpg --export [info-chave]
```

'[info-chave]' é uma informação que permite distinguir sem ambiguidade o par de chaves do qual você quer extrair a chave pública. Se esta informação não é fornecida então são as chaves públicas de todos os pares de chaves e sua frase que serão publicados. Certamente, se você não possui senão um par de chave, nenhuma informação é necessária extrair dela a chave pública.

O comando '—export' escreve a chave pública em caracteres codificados de 8 bits, o que coloca alguns problemas para enviá-la por e-mail ou para mostrá-la. A opção '—armor' ou '—a' permite obter uma chave pública em caracteres codificados de 7 bits.

Por padrão, a chave pública é escrita na saída padrão. A opção '—output' ou '—o' permite escrever essa chave num arquivo e não na saída padrão do sistema.

Uma vez que sua chave pública está num arquivo, você deve colocá-la à disposição de seus eventuais interlocutores para que eles possam se dela servir para enviar mensagens criptografadas com a mesma. Você pode fazê-lo, por exemplo, colocando esta chave

numa de suas páginas Web, em seu arquivo '~/.plan', enviando-a por e-mail ou colocando num servidor de chaves.

3.3 Como acrescentar uma chave pública ao seu chaveiro digital?

Para poder usar a chave pública de um de seus interlocutores, você deve acrescentá-la ao seu chaveiro digital com o comando '--import':

```
gpg --import [arquivo]
```

Se nenhum nome de arquivo é posto no parâmetro, a chave pública é lida a partir da entrada padrão.

3.4 Como publicar o conteúdo do seu chaveiro digital?

O comando '--list-keys' envia todas as chaves públicas que você possui e todas as informações anexadas às suas suas chaves públicas para saída padrão:

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

Você pode obter as assinaturas públicas que possui com o comando '--list-sigs':

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

e as chaves privadas de seu molho com o comando '--list-secret-keys':

```
gpg --list-secret-keys
```

3.5 Como retirar chaves do seu chaveiro digital?

O comando '--delete-key' permite apagar uma chave pública de seu chaveiro digital:

```
gpg --delete-key info-chave
```

e o comando '`--delete-secret-key`' permite apagar uma chave privada de seu chaveiro digital:

```
gpg --delete-secret-key
```

3.6 Como publicar a 'impressão digital' (fingerprint) de uma chave pública de seu chaveiro digital?

O comando '`--fingerprint`' mostra as 'impressões digitais' das chaves públicas de seu chaveiro digital:

```
gpg --fingerprint
```

3.7 Como assinar uma chave pública de seu chaveiro digital?

Como vimos na introdução, a autenticidade das chaves públicas de seu chaveiro digital é essencial para a segurança de sua correspondência criptografada. Para estar seguro da autenticidade de novas chaves públicas, você pode utilizar as assinaturas dessas chaves. Você pode igualmente dar garantias da autenticidade de certas chaves públicas assinando-as com uma de suas chaves privadas graças ao comando '`--edit-key`':

```
gpg --edit-key info-chave
```

Este comando vai dar acesso a um menu textual que permite ao usuário, entre outras coisas, a assinar a chave designada por '`info-chave`' digitando '`sign`'. Uma vez a chave publicada, você pode torná-la pública da mesma forma que para uma de suas chaves públicas. Ainda uma vez, lembremos que você pode totalmente comprometer a segurança de suas correspondências e daqueles que você confia, ao dar levemente confiança. Portanto, somente assine uma chave pública quando você está **ABSOLUTAMENTE CERTO** da autenticidade da chave que você está assinando.

Esse menu textual permite também modificar o nível de confiança com o comando '`trust`'. Os níveis de confiança são:

- * 1 = Eu não sei (I don't know)
- * 2 = Eu não confio (I do NOT trust)
- * 3 = Eu tenho pouca confiança (I trust marginally)
- * 4 = Eu tenho confiança total (I trust fully)

Esses níveis de confiança são usados quando da verificação da assinatura de uma mensagem. Com efeito, se você não tem nenhuma ou mesmo pouca confiança numa chave pública, a validade de uma assinatura baseada sobre esta chave pública não pode garantir a autenticidade da mensagem.

3.8 Como gerar um certificado de revogação para um de seus pares de chaves?

Você pode gerar um certificado de revogação para um par de chaves que esteja em sua posse a qualquer instante com o comando '`--gen-revoke`':

```
gpg --gen-revoke info-chave
```

Atenção, a geração de um certificado de revogação de um par de chaves necessita do conhecimento da chave privada do par a ser revogado. Se você esquece a frase-chave de uma de suas chaves, você não poderá revogar este par. Portanto, você tem o interesse desse ponto de vista em gerar esse certificado desde que cria um par. Por outro lado, se alguém consegue obter esse certificado, pode fazer crer que você revogou o par de chaves descrito por esse certificado. Você deverá portanto pôr esse certificado em segurança

3.9 Como modificar uma chave pública do seu chaveiro digital?

O comando '`--edit-key`' dá acesso a menu com vários itens que permite modificar algumas informações associadas a uma chave pública do seu chaveiro digital:

```
gpg --edit-key info-chave
```

Você pode conhecer os comandos acessíveis neste menu com o comando '`help`'.

4. Criptografar e descriptografar

A operação de criptografia ou cifragem produz uma mensagem em caracteres de 8-bits, o que coloca alguns problemas para enviá-lo por e-mail ou para publicá-lo. A opção '`--armor`' ou '`-a`' permite a produção de um arquivo de de 7-bits.

Por padrão, as operações de criptografar e descriptografar mostram seus resultados na saída padrão. A opção '--output' ou '-o' permite escrever o resultado dessas operações num arquivo e não na saída padrão do sistema.

4.1 Como criptografar uma mensagem?

Para criptografar uma mensagem, você deve dispor da chave pública de quem se destina a mensagem. Esse último utilizará em seguida sua chave privada para descriptografar a sua mensagem. Você deve portanto precisar o destinatário da mensagem, ou para ser mais preciso da chave pública a ser utilizada, quando de uma cifração:

```
gpg --encrypt destinatário [mensagem]
```

ou

```
gpg -e destinatário [mensagem]
```

'Destinatário' representa aqui toda informação que permite distinguir sem ambiguidade uma chave pública entre todas as chaves públicas de seu chaveiro digital. Esta informação pode ser, por exemplo, o nome ou o endereço de e-mail associado à chave pública que você deseja utilizar. Você pode mesmo fornecer somente uma parte do nome ou do endereço de e-mail se esta parte baste para distinguir uma chave pública sem ambiguidade.

Para evitar que alguém possa usurpar sua identidade, aconselha-se assinar toda mensagem que você criptografa.

4.2 Como descriptografar uma mensagem?

Como a decifração ou descriptografia utiliza sua chave privada e você não tem senão uma regra geral, não é necessário precisá-la:

```
gpg [--decrypt] [mensagem]
```

ou

```
gpg [-d] [mensagem]
```

Se você possui várias chaves privadas, deve precisar a chave privada a ser utilizada para a decifragem com a opção '--local-user info-chave' ou '-u info-chave'. 'Info-chave' é toda informação que permite distinguir sem ambiguidade uma chave privada entre todas as suas chaves privadas.

5. Assinar e verificar assinaturas

Assim como para a cifragem, assinar uma mensagem produz uma assinatura em caracteres de 8-bits, o que pode gerar alguns problemas para enviá-la por e-mail ou para publicá-la. Aí ainda, a opção '--armor' ou '-a' permite a produção de uma assinatura em caracteres de 7-bits.

A opção '--output' ou '-o' permite também escrever o resultado da operação de assinatura num arquivo e não na saída padrão do sistema.

5.1 Como assinar uma mensagem?

O comando '--sign' (ou '-s') permite assinar uma mensagem:

```
gpg --sign [mensagem]
```

O comando '--sign' ao mesmo tempo assina e compacta a mensagem. Se você não quer compactar o resultado, pode simplesmente acrescentar uma assinatura no fim da mensagem graças ao comando '--clearsign':

```
gpg --clearsign [mensagem]
```

Os dois comandos precedentes remetem a mensagem seguida da assinatura. Se apenas a assinatura interessa, você pode utilizar o comando '--detach-sign' (ou '-b'):

```
gpg --detach-sign [mensagem]
```

Este comando é particularmente útil para assinar arquivos de dados binários ou executáveis.

Você pode igualmente assinar e criptografar uma mensagem numa única operação:

```
gpg [-u remetente] [-r destinatário] [--armor] --sign --encrypt [mensagem]
```

5.2 Como verificar a assinatura de uma mensagem?

Quando uma mensagem é criptografada, ela é igualmente assinada e esta assinatura é automaticamente verificada quando da decifragem (certamente, apenas se você dispor da chave pública do signatário). Você pode também apenas se contentar em verificar a assinatura de uma mensagem:

```
gpg --verify [mensagem]
```

Esta verificação se apoiando na chave pública associada à chave privada tendo servido à assinar a mensagem, você deve com certeza dispor desta chave pública. No entanto, esta verificação somente é válida na medida em que você dedica um cuidado especial à verificação da autenticidade das chaves públicas que utiliza.

6. Documentações suplementares

6.1 GnuPG

- * O site oficial do GnuPG
- * As listas de discussão do GnuPG acessíveis no site oficial, compreendendo seus arquivos e descrições.
- * Uma documentação completa é em curso de redação. A versão mais atualizada está disponível no site oficial.
- * A documentação integrada ao gpg é seguramente a de mais simples acesso:

```
gpg --help
```

6.2 PGP

PGP é um programa mais antigo e mais difundido de criptografia. Numerosas documentações utilizáveis também para o GnuPG foram escritas nos cursos desses anos e você pode, em particular, consultar:

- * O site internacional do PGP
- * O FAQ PGP DH em relação ao RSA (este FAQ representa as diferenças entre dois algoritmos utilizados pelo GnuPG).

6.3 Servidores de chaves

- * <http://www.keyserver.net>
- * <http://wwwkeys.eu.pgp.net>
- * <http://www.es.net/hypertext/pgp>
- * <http://pgp.zdv.uni-Mainz.de/keyserver>
- * <http://pgp.yashy.com>

6.4 Livros

- * B. Schneier. *Criptografia Aplicada*. Segunda Edição, Wiley and International Thomson Publishing, 1997.

No Brasil:

- * Daniel Balparda de Carvalho. *Segurança de Dados com Criptografia. Métodos e Algoritmos*. Rio de Janeiro, Editora Book Express, 2000.

7. Versões deste documento

7.1 Esclarecimentos sobre a versão inglesa

Original German versions: Version 0.1 was the first version in German

Changes in version 0.1.1 (German)

- * New section "Boudaries to security"
- * Improved explanation of signatures
- * Changes after comments from Werner Koch (thanks!)

All changes are documented in a diff file: dieses Dokument

For the english version: All remarks for this document can be send to Brenno J. S. A. A. F. de Winter (brenno@dewinter.com). Comments help us make a better document and are greatly appreciated. For the german version: Anregungen, Kritik, Verbesserungen und Erweiterungen eifach an Michael Fischer v. Mollard (fischer@math.uni-goettingen.de) senden, damit dieses Dokument weiter verbessert werden kann.

* English version 0.1.0 April 30th 1999, Duth Queen's Day. This version is the translation of the german version in English with some adjustments.

7.2 Esclarecimentos sobre a versão francesa

Cette version est en grande partie basée sur la version anglaise (merci à Brenno *8)) même si ce n'est pas une traduction mot à mot. J'ai un peu modifié la structure de la première et de la troisième partie de ce document. J'ai aussi un peu modifié le contenu de la première partie.

Ce document n'en est qu'à sa première version et attend vos remarques, vos suggestions et surtout vos ajouts pour s'améliorer. Si vous me les faites parvenir, je pourrai les intégrer aux versions futures de ce document et ainsi faire profiter le plus grand nombre de vos lumières *8)

dindart@labri.u-bordeaux.fr

* Version Française 0.1.0 du 10 octobre 1999. Cette version est une traduction légèrement remaniée de la version anglaise 0.1.0.

7.3 Esclarecimentos sobre a versão brasileira

Esta versão foi feita a partir da tradução francesa 0.1.0, com algumas pequenas comparações com a versão inglesa 0.1.0.

Esta tradução nada acrescentou ao texto francês, exceto uma referência bibliográfica, e outros endereços de servidores de chaves.

Espero trazer melhorias futuramente ao texto, e espero contribuições de todos que querem desenvolver o uso do GnuPG em particular, e também do Software Livre em nosso país. Qualquer um pode me contactar no seguinte e-mail:

rmartini@cipsga.org.br

para informações sobre futuras versões procure:

<http://www.cipsga.org.br>

Espero críticas, sugestões, melhorias, etc.

Uma nota a respeito de certos termos:

Use cifragem e criptografar e seus derivados como sinônimos. Neste documento não é utilizado o termo "encriptar" e derivados.

"Chaveiro digital" é a solução que encontrei para a palavra "keyring", literalmente chaveiro... A tradução francesa usa "trousseau", que poderia em contrapartida ser traduzido por "molho de chaves", ficamos entretanto com chaveiro.

"Impressão digital" é a tradução de "fingerprint", 'marca' em hexadecimal que singulariza uma chave.

* Versão Brasileira 0.1 de 18 de junho de 2000. Esta é uma tradução da versão francesa 0.1.0

Controle da versão em Português

<i>Data</i>	<i>Tradutor</i>	<i>Observações</i>
18/06/2000	Renato Martini	Tradução inicial em Português

GNU Free Documentation License

Version 1.1, March 2000

Copyright (C) 2000 Free Software Foundation, Inc.
59 Temple Place, Suite 330, Boston, MA 02111-1307 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

0. PREAMBLE

The purpose of this License is to make a manual, textbook, or other written document "free" in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or noncommercially. Secondly, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of "copyleft", which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

1. APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. The "Document", below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as "you".

A "Modified Version" of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A "Secondary Section" is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (For example, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The "Invariant Sections" are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License.

The "Cover Texts" are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License.

A "Transparent" copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, whose contents can be viewed and edited directly and straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup has been designed to thwart or discourage subsequent modification by readers is not Transparent. A copy that is not "Transparent" is called "Opaque".

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML designed for human modification. Opaque formats include PostScript, PDF, proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for

which the DTD and/or processing tools are not generally available, and the machine-generated HTML produced by some word processors for output purposes only.

The "Title Page" means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page.

For works in formats which do not have any title page as such, "Title Page" means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.

2. VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

3. COPYING IN QUANTITY

If you publish printed copies of the Document numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a publicly-accessible computer-network location containing a complete Transparent copy of the Document, free of added material, which the general network-using public has access to download anonymously at no charge using public-standard network protocols. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

4. MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

- A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.
- B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has less than five).

- C. State on the Title page the name of the publisher of the Modified Version, as the publisher.
- D. Preserve all the copyright notices of the Document.
- E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.
- F. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.
- G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.
- H. Include an unaltered copy of this License.
- I. Preserve the section entitled "History", and its title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.
- J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.
- K. In any section entitled "Acknowledgements" or "Dedications", preserve the section's title, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.
- L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.
- M. Delete any section entitled "Endorsements". Such a section may not be included in the Modified Version.
- N. N. Do not retitle any existing section as "Endorsements" or to conflict in title with any Invariant Section.
- O. If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.

You may add a section entitled "Endorsements", provided it contains nothing but endorsements of your Modified Version by various parties—for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

5. COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections entitled "History" in the various original documents, forming one section entitled "History"; likewise combine any sections entitled "Acknowledgements", and any sections entitled "Dedications". You must delete all sections entitled "Endorsements."

6. COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

7. AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, does not as a whole count as a Modified Version of the Document, provided no compilation copyright is claimed for the compilation. Such a compilation is called an "aggregate", and this License does not apply to the other self-contained works thus compiled with the Document, on account of their being thus compiled, if they are not themselves derivative works of the Document. If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one quarter of the entire aggregate, the Document's Cover Texts may be placed on covers that surround only the Document within the aggregate. Otherwise they must appear on covers around the whole aggregate.

8. TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires especial permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License provided that you also include the original English version of this License. In case of a disagreement between the translation and the original English version of this License, the original English version will prevail.

9. TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly provided for under this License. Any other attempt to copy, modify, sublicense or distribute the Document is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

10. FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See <http://www.gnu.org/copyleft/>.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License "or any later version" applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation.

How to use this License for your documents.

To use this License in a document you have written, include a copy of the License in the document and put the following copyright and license notices just after the title page:

Copyright (c) YEAR YOUR NAME.

Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.1 or any later version published by the Free Software Foundation; with the Invariant Sections being LIST THEIR TITLES, with the Front-Cover Texts being LIST, and with the Back-Cover Texts being LIST. A copy of the license is included in the section entitled "GNU Free Documentation License".

If you have no Invariant Sections, write "with no Invariant Sections" instead of saying which ones are invariant. If you have no Front-Cover Texts, write "no Front-Cover Texts" instead of "Front-Cover Texts being LIST"; likewise for Back-Cover Texts.

If your document contains nontrivial examples of program code, we recommend releasing these examples in parallel under your choice of free software license, such as the GNU General Public License, to permit their use in free software.

Comitê de Incentivo a Produção do Software Gratuito e Alternativo



Fundado em 29 de janeiro de 1999.

1ª Diretoria

Djalma Valois Filho

Diretor Executivo

dvalois@cxpostal.com

José Luiz Nunes Poyares
Diretor Administrativo

Paulo Roberto Ribeiro Guimarães
Diretor Institucional

CIPSGA
Rua Professora Ester de Melo, numero 202,
Parte, Benfica, Rio de Janeiro, RJ, CEP. 20930-010;
Telefone (Fax/Dados): 021-5564201;
e-mail: administracao@cipsga.org.br
CNPJ: 03179614-0001/70