

EasyPG Assistant

by Daiki Ueno

これは EasyPG アシスタント1.0.0 の説明書です。

Copyright © 2007--2025 Free Software Foundation, Inc.

Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.3 or any later version published by the Free Software Foundation; with no Invariant Sections, with the Front-Cover Texts being “A GNU Manual,” and with the Back-Cover Texts as in (a) below. A copy of the license is included in the section entitled “GNU Free Documentation License”.

この文書を、フリーソフトウェア財団発行の GNU フリー文書利用許諾契約書第 1.3 版またはそれ以降の版が定める条件の下で複製、配布、あるいは変更することを許可します。変更不可部分は指定しません。“A GNU Manual”は表表紙テキスト、以下の(a) は裏表紙テキストです。この利用許諾契約書の複写は「GNU フリー文書利用許諾契約書」という章に含まれています。

(a) The FSF’s Back-Cover Text is: “You have the freedom to copy and modify this GNU manual.

(a) FSF の裏表紙テキスト: 「あなたにはこの GNU Manual を複製したり変更する自由があります。」

目次

1	概要.....	1
2	とりあえず始める	2
3	コマンド	3
3.1	鍵の管理	3
3.2	領域の暗号や署名の操作	4
3.3	ファイルの暗号や署名の操作	5
3.4	Dired の統合	5
3.5	Mail モードの統合	5
3.6	gpg ファイルの暗号化と復号	6
3.7	Querying a key server	8
4	GnuPG のバージョンの互換性.....	9
5	GnuPG Pinentry	10
6	Caching Passphrases	11
7	バグリポート	12
	付録 A GNU Free Documentation License.....	13
	Concept Index	21
	Key Index	22
	Function Index.....	23
	Variable Index.....	24

1 概要

EasyPG アシスタントはGnuPG (GNU Privacy Guard) の Emacs フロントエンド・アプリケーションです。以下の機能を提供します:

- 鍵の管理
- 領域の暗号や署名の操作
- ファイルの暗号や署名の操作
- Dired の統合
- Mail モードの統合
- *.pgp ファイルの自動暗号化/復号

2 とりあえず始める

EasyPG アシスタントは Emacs や GnuPG の設定を何もしなくても使うことができます。例えば対称鍵暗号を使ってファイルを自動的に暗号化したり復号化できます。Section 3.6 [Encrypting/decrypting gpg files], p. 6, を参照してください。ただし EasyPG アシスタントの機能の完全なセットを使うには、少なくとも最少限の GnuPG の適切な設定が必要です。

John Michael Ashley の GNU プライバシー・ハンドブックはオンラインでthe GnuPG user guides (<https://gnupg.org/documentation/guides.html>) の一部として入手可能で、GnuPG の使いかたと設定の入門方法を提供しています。それとは対照的に、GnuPG マニュアル(see *Using the GNU Privacy Guard*) はより詳しいリファレンスマニュアルのようなものです。

EasyPG アシスタント・コマンドは‘epa-’で始まります。例えば、

- 鍵リングを眺めるには `M-x epa-list-keys`
- 領域のクリアテキスト署名を作るには `M-x epa-sign-region`
- ファイルを暗号化するには `M-x epa-encrypt-file`
- キーサーバーにキーを問い合わせるには `M-x epa-search-keys`

EasyPG アシスタントは Emacs の他の機能性に統合することができるいくつかの暗号や署名の機能を提供します。例えば*.gpg ファイルの暗号化と復号です。

3 コマンド

この章は代表的な使い方のための様々なコマンドを紹介します。

3.1 鍵の管理

おそらく EasyPG アシスタントを使う最初の一步は鍵リングを眺めることでしょう。*M-x epa-list-keys* はコマンドラインから使う `'gpg--list-keys'` に相当しています。

epa-list-keys name mode [Command]

公開鍵リングの *name* に合致するすべての鍵を表示します。

その出力は次のようなものです。

```
u A5B6B2D4B15813FE Daiki Ueno <ueno@unixuser.org>
```

左端の桁の文字はその鍵の信頼度を表します。もし `'u'` ならば、その鍵は究極的に信頼されるものとして印されています。二つ目の桁はその鍵の ID、残りはユーザー ID です。

TAB で項目を移動できます。ある項目で RET をタイプするかマウスの第 1 ボタンをクリックすると、選択した鍵のもっと詳細な情報を見ることができます。

```
u Daiki Ueno <ueno@unixuser.org>
u A5B6B2D4B15813FE 1024bits DSA
    Created: 2001-10-09
    Expires: 2007-09-04
    Capabilities: sign certify
    Fingerprint: 8003 7CD0 0F1A 9400 03CA  50AA A5B6 B2D4 B158 13FE
u 4447461B2A9BEA2D 2048bits ELGAMAL_E
    Created: 2001-10-09
    Expires: 2007-09-04
    Capabilities: encrypt
    Fingerprint: 9003 D76B 73B7 4A8A E588  10AF 4447 461B 2A9B EA2D
```

秘密鍵リングを眺めるには *M-x epa-list-secret-keys* を使ってください。

epa-list-secret-keys name [Command]

秘密鍵リングの中の *name* に合致するすべての鍵を表示します。

Keys バッファではいくつかのコマンドを利用できます。よくある用途はいくつかの鍵をファイルに書き出すことです。それには *m* をタイプして鍵を選択し、*o* をタイプした後でファイル名を入力してください。

以下は鍵の管理に関する他のコマンドです。それらのいくつかはファイルを対象に入出力を行ない、他は現在設定されている領域が対象になります。

epa-insert-keys keys [Command]

カーソルの後ろに選択された *keys* を挿入します。挿入する前に鍵を選択することを促されます。デフォルトでは鍵を OpenPGP の装甲フォーマットでエンコードします。

epa-import-keys file [Command]

鍵を *file* から鍵リングに取り込みます。

`epa-import-keys-region start end` [Command]
 鍵を *start* と *end* の間の現在の領域から鍵リングに取り込みます。

`epa-import-armor-in-region start end` [Command]
 鍵を *start* と *end* の間の現在の領域にある OpenPGP の装甲フォーマットから鍵リングに取り込みます。`epa-import-keys-region` との違いは `epa-import-armor-in-region` が領域にある装甲を探して、それらを逐一 `epa-import-keys-region` が処理することです。

`epa-delete-keys allow-secret` [Command]
 選択された鍵を取り除きます。`allow-secret` が `nil` でなかったら秘密鍵も取り除きます。

3.2 領域の暗号や署名の操作

`epa-decrypt-region start end` [Command]
start と *end* の間の現在の領域を復号します。復号されたテキストで領域を置き換えます。

`epa-decrypt-armor-in-region start end` [Command]
start と *end* の間の現在の領域にある OpenPGP 装甲を復号します。`epa-decrypt-region` との違いは `epa-decrypt-armor-in-region` が領域にある装甲を探して、それらを逐一 `epa-decrypt-region` が処理することです。したがってこのコマンドは装甲の前後にある元のテキストを改変しません。

`epa-verify-region start end` [Command]
start と *end* の間の現在の領域を検証します。検証結果はミニバッファークポップアップされるウィンドウに送ります。領域を署名されたテキストで置き換えます。

`epa-verify-cleartext-in-region` [Command]
start と *end* の間の現在の領域にある OpenPGP のクリアテキスト・ブロックを検証します。`epa-verify-region` との違いは `epa-verify-cleartext-in-region` が領域にあるクリアテキスト・ブロックを探して、それらを逐一 `epa-verify-region` が処理することです。したがってこのコマンドはクリアテキスト・ブロックの前後にある元のテキストを改変しません。

`epa-sign-region start end signers type` [Command]
start と *end* の間の現在の領域に署名します。デフォルトではクリアテキストの署名を作ります。接頭引数を与えると署名に使う鍵と署名のタイプを選択することを促されます。

`epa-encrypt-region start end recipients sign signers` [Command]
start と *end* の間の現在の領域を暗号化します。受取人を選択することを促されます。接頭引数を与えると暗号化する前にテキストに署名するかどうかを尋ねられ、`yes` と答えた場合は署名に使う鍵を選択することを促されます。

`epa-keys-select-method` [変数]
 この変数は `epa-select-keys` で鍵の選択に使う方法を指定します。デフォルト値 `buffer` を指定すると、鍵を選択できる特別なバッファークポップアップします。値を `minibuffer` にすると、`epa-select-keys` は代わりにミニバッファーク内で鍵の入力を求めます。鍵はカンマで区切って入力しなければなりません。

3.3 ファイルの暗号や署名の操作

epa-decrypt-file *file* &optional *output* [Command]
file を復号します。もし複合した結果を格納するファイルの名前を *output* で指定しないと、それを入力することを求めます。

epa-verify-file *file* [Command]
file を検証します。

epa-sign-file *file* *signers* *type* [Command]
file に署名します。接頭引数を与えると署名に使う鍵と署名のタイプを選択することを促されます。

epa-encrypt-file *file* *recipients* [Command]
file を暗号化します。受取人を選択することを促されます。

3.4 Dired の統合

EasyPG アシスタントは GNU Emacs の dired モードを拡張して、ファイルの暗号や署名の操作ができるようにします。例えば次のようなことができます。

```
M-x dired
(いくつかのファイルに選択マークを付けて)
: e (or M-x epa-dired-do-encrypt)
(`m' で受取人を選択して [OK] をクリック)
```

以下のキーが割り当てられています。

```
: d      マークされたファイルを復号します。
: v      マークされたファイルを検証します。
: s      マークされたファイルに署名します。
: e      マークされたファイルを暗号化します。
```

3.5 Mail モードの統合

EasyPG アシスタントはインライン OpenPGP メッセージの作成を支援するためにマイナーモード **epa-mail-mode** を提供します。インライン OpenPGP メッセージは、現代的な MIME フォーマットを使わずに生の OpenPGP blobs (バイナリーデータ) をメッセージの本体に埋め込むことによって、署名をしたり暗号化した電子メールを送る伝統的な形式です。

注: インライン OpenPGP は推奨されません。PGP/MIME を使うことを考えるべきです。Inline OpenPGP in E-mail is bad, Mm'kay? (<https://josefsson.org/inline-openpgp-considered-harmful.html>) を参照してください。

epa-mail-mode を有効にすると以下のキーが割り当てられます。このマイナーモードを有効にするには **C-u 1 M-x epa-mail-mode** を実行するか、カスタムのインターフェースを通して行なってください(**M-x customize-variable epa-global-mail-mode** を試してください)。

```
C-c C-e C-d and C-c C-e d
現在のバッファにある OpenPGP 装甲を復号します。
```


C-c C-e C-v and C-c C-e v

現在のバッファにある OpenPGP のクリアテキストで署名されたメッセージを検証します。もし何らかの理由で検証が失敗する場合、このコマンドはエラーを発生します。

C-c C-e C-s and C-c C-e s

デフォルトの鍵を使って現在のバッファから署名されたメッセージを作ります。接頭引数を与えると鍵を対話的に選ぶことができます。

C-c C-e C-e and C-c C-e e

現在のバッファから暗号化されたメッセージを作ります。デフォルトではメールのヘッダーの‘to’、‘cc’、および‘bcc’ フィールドから受取人リストを作ろうとします。受取人リストにあなたの鍵を含めたい場合は `~/.gnupg/gpg.conf` で `‘encrypt-to’` オプションを使ってください。この関数は `epa-mail-aliases` リストを使って受取人アドレスを書き換えます。そのオプションを特定の受取人を暗号化の対象としないために使うこともできます。

接頭引数を与えると、受取人の選択、署名するかどうか、およびどの鍵で署名するかを対話的に指示することができます。

3.6 gpg ファイルの暗号化と復号

デフォルトでは名前が `.gpg` で終わるファイルは暗号化されたものとして扱われます。即ちそのようなファイルを開くと、暗号化されたままのものではなく復号されたテキストがバッファに挿入されます。同様にバッファを `foo.gpg` ファイルにセーブすると暗号化されたデータが書かれます。

初めてバッファを暗号化ファイルに保存しようとする、EasyPG アシスタントはバッファ*Keys*にある鍵のリストを表示して、そこで暗号化する対象の受信者を選択することができます。バッファの形式の説明については See Section 3.1 [Key management], p. 3. この受信者を選択する手順は、この章で後述する変数 `epa-file-encrypt-to` および `epa-file-select-keys` をカスタマイズすることによって効率化することができます。

この段階で受信者を選択しない場合、EasyPG アシスタントは対称鍵暗号を使います。その結果、バッファを保存するたびにパスフレーズを2回入力しなければならないし、ファイルを読み取るときにも頻繁にパスフレーズの入力が必要になります。それは、GnuPG エージェントは、少なくともしばらくの間ファイル読み取り用にパスフレーズをキャッシュしますが、バッファの保存用にはキャッシュしないからです。より多くの情報は See Chapter 6 [Caching Passphrases], p. 11.

自分で鍵の対を作った場合¹、それは受信者として選択することができ、EasyPG アシスタントはそのファイルに公開鍵暗号を使用します。GnuPG は公開鍵を使って暗号化を実行するので、バッファ保存の場合はパスフレーズの入力を求められませんが、GnuPG エージェントのキャッシュ設定に応じて、ファイル読み取りの場合はパスフレーズの入力を求められることがあります。

上述のように、ファイルを暗号化および復号するために EasyPG アシスタントはある特定の状況の下では、処理するファイルのプレーンテキスト・コンテンツを含む一時的な中間ファイルを使います。EasyPG アシスタントは、関数 `temporary-file-directory` (see

¹ 共有する予定のないファイルを暗号化および復号するときは、鍵の対を作る際に受信者として電子メールアドレスを使用する必要はありません。`backup` や `account database` など、鍵の対の用途に関する情報を提供する自由形式の文字列を使うこともできます。

Section “Generating Unique File Names” in *GNU Emacs Lisp Reference Manual*) が返すディレクトリーの下にそれらを作成します。プレーンテキストの痕跡を残したくないのであれば、少なくともそのディレクトリーでは暗号化されたファイルシステムを使用してください。

暗号化されたファイルの名前パターンは`epa-file-name-regexp` で制御することができます。

epa-file-name-regexp [変数]

暗号化されたものとして扱われるファイル名に合致する正規表現です。

この動作は`M-x epa-file-disable` で無効に、そして`M-x epa-file-enable` で元に戻すことができます。

epa-file-disable [Command]

`*.gpg` ファイルの自動暗号化/復号を無効にします。

epa-file-enable [Command]

`*.gpg` ファイルの自動暗号化/復号を有効にします。

デフォルトでは`epa-file` は対称鍵暗号(symmetric encryption)、言い換えるとパスワードに基づいた暗号を使おうとします。代わりに公開鍵暗号(public key encryption) を使いたいのであれば`M-x epa-file-select-keys` を行なってください。するとキーを選択するための対話窓がポップアップします。

epa-file-select-keys [Command]

現在開いているファイルを公開鍵で暗号化するための受取人の鍵を選択します。

変数`epa-file-select-keys` でデフォルトの動作を変更することもできます。

epa-file-select-keys [変数]

鍵を選択するための対話窓をポップアップするかどうかを制御します。

頻繁に開くファイルについては、どの暗号方式を使うべきかをファイル変数(see Section “Local Variables in Files” in *The Emacs Editor*) を介して Emacs に伝えておくことは良い考えかもしれません。この目的にはローカル変数`epa-file-encrypt-to` を使ってください。

例えば ELisp ファイルを電子メールアドレス‘`ueno@unixuser.org`’ に対応する公開鍵暗号で暗号化したいのであれば、そのファイルの先頭に以下の行を加えてください。

```
;; -*- epa-file-encrypt-to: ("ueno@unixuser.org") -*-
```

逆にファイルを常に(`epa-file-select-keys` 変数の値に関わらず) 対称鍵暗号で暗号化したいのであれば、その行を以下のように変更してください。

```
;; -*- epa-file-encrypt-to: nil -*-
```

自動暗号化/復号の動作を制御する他の変数は以下の通りです。

epa-file-cache-passphrase-for-symmetric-encryption [変数]

`nil` 以外の値だったら対称鍵暗号のためのパスフレーズをキャッシュします。デフォルト値は`nil` です。

安全上の理由から、このオプションはデフォルトでオフになっていて、使うことを推奨しません。代わりに、多くの場合同じ仕事をより安全な方法で行なうことができる GnuPG エージェントを使うことを考慮してください。詳細については、See Chapter 6 [Caching Passphrases], p. 11.

epa-file-inhibit-auto-save [変数]
nil 以外の値だったら開いている暗号化されたファイルの自動セーブを禁止します。
デフォルト値はt です。

3.7 Querying a key server

epa-search-keys コマンドを使って、GPG キーサーバーに問い合わせることができます。その際 Emacs は合致するものを一覧できるバッファをポップアップし、そこで個人のキーリングにキーを取り込む(および追加する) ことができます。

そのキーの検索結果を表示するバッファでは、**f** コマンドを使ってキーを取り込むようにマークしてから**x** を使ってキーを取り込んで(およびキーリングに組み込んで) ください。

変数**epa-keyserver** で、どのサーバーに問い合わせるかを指示します。

4 GnuPG のバージョンの互換性

2023 年 6 月現在 GnuPG には 3 つの活動的な枝があります; 2.4、2.2、および 1.4 です。GnuPG バージョン 2.4.1 以降は GnuPG bug T6481 (<https://dev.gnupg.org/T6481>) の影響を受けていて、Emacs ではほとんど使えません。少なくとも GnuPG バージョン 2.4.1 では、そのバグに対するパッチが存在していて、オペレーティングシステムまたはディストリビューションがすでに提供している可能性があります。GnuPG 1.4 はレガシーバージョンとみなされます。

それに加えて、上記のブランチはすべて、基本的なユースケースでは Emacs で問題なく動作するはずです。ただし、Emacs から使うと目に見えるかもしれない互換性のない特徴があります。

- GnuPG 2.1 の鍵を格納するためのフォーマットは 1.4 と異なります。それは GnuPG 2.1 で作成された鍵が 1.4 では見えないかもしれないということです。
- GnuPG 2.1 は `gpg-agent` と通信するために固定アドレスの Unix ドメインソケットを使います。GnuPG 2.0 と 1.4 で使われている `GPG_AGENT_INFO` 環境変数は無視します。このことは、もしあなたのシステムに GnuPG 2.1 と 1.4 の両方があるとすると、GnuPG 1.4 由来の `gpg` コマンドは 2.1 が提供する `gpg-agent` を(少なくともそのままでは) 使えないことを意味します。
- GnuPG 2.1 (2.1.5 以降) は Emacs のミニバッファから直接 Pinentry を入力することができます。See Chapter 5 [GnuPG Pinentry], p. 10.

5 GnuPG Pinentry

GnuPG スイーツの重要な構成要素は Pinentry です。これによって GnuPG が要求するパスフレーズを安全に入力することができます。GnuPG は淡泊な TTY のみの `pinentry-tty` から色々なデスクトップ環境用の華美なグラフィカル・ダイアログ、例えば `pinentry-gnome3` に至るまで、様々なプログラムを Pinentry として提供します。通常はオペレーティングシステムによって、これらのどれがデフォルトで使用されるかが決まります。

具体的な Pinentry プログラムの選択によって、どのくらいの頻度ではなく、どのように GnuPG がパスフレーズを要求するかのみが決定されることに注意してください。後者の質問については Chapter 6 [Caching Passphrases], p. 11, を参照してください。

いくつかの設定を行うと、Emacs は Pinentry の役割を果たすこともできます。GnuPG 2.1.5 以降で利用できる最も自然な選択は、Emacs によってトリガーされるリクエストの Pinentry として Emacs 自体を使用することです。たとえば、名前が `.gpg` で終わるファイルを自動復号化を使用して開く場合、そのリクエストのパスフレーズも Emacs に入力する必要があるでしょう。

このいわゆる *loopback Pinentry* には、Emacs をリモートまたはテキスト専用端末から使用する場合にも機能するという追加の利点があります。有効にするには:

1. オプション `allow-loopback-pinentry` が `gpg-agent` に設定されていることを確認してください。これはデフォルトであるべきです。See Section “Option Summary” in *Using the GNU Privacy Guard*.
2. Emacs で変数 `epg-pinentry-mode` を `loopback` にカスタマイズしてください。

Loopback Pinentry は `gpgsm` では機能しないので、EasyPG はこの設定を無視することに注意してください。

Emacs を Pinentry として使用するために利用できるオプションは他にもあります。 `pinentry-emacs` または `gpg-agent` のオプションである `allow-emacs-pinentry` と呼ばれる Pinentry が見つかるかもしれません。ただし、これらは安全でないか半ば廃れている (semi-obsolete) と考えられていて、オペレーティングシステムやディストリビューションによってはサポートされていない可能性があります。たとえば、Debian GNU/Linux は、上記のループバック Pinentry のみをサポートします。

6 Caching Passphrases

もし同じファイルを開いたり閉じたりする機会が度々あるのであれば、パスフレーズをタイプするのはわずらわしい仕事でしょう。GnuPG と EasyPG アシスタントは、一定の時間に限ってあなたのパスフレーズを記憶する機構を提供します。これらを使うと、パスフレーズを時々入力し直すだけで済みます。しかしながらその設定は少々込み入っています。それは、インストールされている GnuPG の版(see Chapter 4 [GnuPG version compatibility], p. 9)、暗号方式(対称鍵か公開鍵か)、そして GnuPG Agent を使いたいかどうかによるからです。以下にいくつかの設問があります。

1. GnuPG バージョン 1.4 の代わりに 2.0 かそれ以降のものを使いますか?
2. 公開鍵暗号ではなく対称鍵暗号を使いますか?
3. GnuPG Agent を使いたいですか?

あなたの回答に対応する設定は次の通りです。

1	2	3	Configuration
Yes	Yes	Must	GnuPG Agent を使えるようにしてください。
Yes	No	Must	GnuPG Agent を使えるようにしてください。
No	Yes	Yes	Elisp のパスフレーズ・キャッシュを使ってください。
No	Yes	No	Elisp のパスフレーズ・キャッシュを使ってください。
No	No	Yes	GnuPG Agent を使えるようにしてください。
No	No	No	GnuPG Agent 無しではできません。

GnuPG Agent を使えるようにするにはSection “Invoking GPG-AGENT” in *Using the GNU Privacy Guard* の説明に従ってください。

Elisp のパスフレーズ・キャッシュを使うには`epa-file-cache-passphrase-for-symmetric-encryption` 変数に`nil` 以外の値を設定してください。See Section 3.6 [Encrypting/decrypting gpg files], p. 6.

7 バグリポート

EasyPG アシスタントのバグと諸問題は Emacs 開発チームが活発に対処しています。新機能の要望と提案もおおいに歓迎します。M-x `report-emacs-bug` (see Section “Bugs” in *Reporting Bugs*) を使ってください。

バグリポートを書くときは、その問題を再現するための操作を十分過ぎると思うほど詳細に説明してください。さらにそのバグを修正するために必要な情報を以下のように集めてください。

- GnuPG のバージョン。‘`gpg --version`’ が示すものです。
- GnuPG の設定。~/.gnupg/gpg.conf の中身です。

バグを知らせる前に ~/.emacs ファイルで `epg-debug` 変数に `nil` 以外の値を設定して、そのバグを再度確認してください。そして `*epg-debug*` バッファの中身を含めてください。バッファ名の最初の文字は空白であることに注意してください。

付録 A GNU Free Documentation License

Version 1.3, 3 November 2008

Copyright © 2000, 2001, 2002, 2007, 2008 Free Software Foundation, Inc.

<http://fsf.org/>

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 functional and useful 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 non-commercially. 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, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The “Document”, below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as “you”. You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

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. (Thus, 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. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

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 Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A “Transparent” copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document 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, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. 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, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include 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, PostScript or PDF 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.

The “publisher” means any person or entity that distributes copies of the Document to the public.

A section “Entitled XYZ” means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as “Acknowledgements”, “Dedications”, “Endorsements”, or “History”.) To “Preserve the Title” of such a section when you modify the Document means that it remains a section “Entitled XYZ” according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

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 (or copies in media that commonly have printed covers) 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 computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. 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 fewer than five), unless they release you from this requirement.
 - 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", Preserve 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. For any section Entitled "Acknowledgements" or "Dedications", Preserve the Title of the section, 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. Do not retitle any existing section to be Entitled "Endorsements" or to conflict in title with any Invariant Section.
 - O. Preserve any Warranty Disclaimers.

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, and that you preserve all their Warranty Disclaimers.

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, is called an “aggregate” if the copyright resulting from the compilation is not used to limit the legal rights of the compilation’s users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which 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 half of the entire aggregate, the Document’s Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket 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 special 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, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled “Acknowledgements”, “Dedications”, or “History”, the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

9. TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, or distribute it is void, and will automatically terminate your rights under this License.

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, receipt of a copy of some or all of the same material does not give you any rights to use it.

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. If the Document specifies that a proxy can decide which future versions of this License can be used, that proxy’s public statement of acceptance of a version permanently authorizes you to choose that version for the Document.

11. RELICENSING

“Massive Multiauthor Collaboration Site” (or “MMC Site”) means any World Wide Web server that publishes copyrightable works and also provides prominent facilities for anybody to edit those works. A public wiki that anybody can edit is an example of such a server. A “Massive Multiauthor Collaboration” (or “MMC”) contained in the site means any set of copyrightable works thus published on the MMC site.

“CC-BY-SA” means the Creative Commons Attribution-Share Alike 3.0 license published by Creative Commons Corporation, a not-for-profit corporation with a principal place of business in San Francisco, California, as well as future copyleft versions of that license published by that same organization.

“Incorporate” means to publish or republish a Document, in whole or in part, as part of another Document.

An MMC is “eligible for relicensing” if it is licensed under this License, and if all works that were first published under this License somewhere other than this MMC, and subsequently incorporated in whole or in part into the MMC, (1) had no cover texts or invariant sections, and (2) were thus incorporated prior to November 1, 2008.

The operator of an MMC Site may republish an MMC contained in the site under CC-BY-SA on the same site at any time before August 1, 2009, provided the MMC is eligible for relicensing.

ADDENDUM: 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 1.3
or any later version published by the Free Software Foundation;
with no Invariant Sections, no Front-Cover Texts, and no Back-Cover
Texts. A copy of the license is included in the section entitled ``GNU
Free Documentation License''.
```

If you have Invariant Sections, Front-Cover Texts and Back-Cover Texts, replace the “with...Texts.” line with this:

```
with the Invariant Sections being list their titles, with
the Front-Cover Texts being list, and with the Back-Cover Texts
being list.
```

If you have Invariant Sections without Cover Texts, or some other combination of the three, merge those two alternatives to suit the situation.

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.

Concept Index

A

automatic file encryption and decryption 6

B

browse key ring 3
bug reports 12

C

caching passphrases 11
compatibility with gnupg 9
configuration of gnupg 2
cryptographic operations on files 5
cryptographic operations on regions 4

D

decrypt file 5
decrypt region 4
decrypting gpg files 6
delete keys 4
directory operations 5
dired integration 5
documentation on gnupg 2

E

encrypt file 5
encrypt region 4
encrypting gpg files 6
entering passphrases 11

F

features of easypg assistant 1
file operations, cryptographic 5

G

gnupg documentation 2
gnupg pinentry 10
gnupg version compatibility 9
gpg files, encrypting and decrypting 6

I

import keys 3
insert keys 3
introduction to easypg assistant 2
introduction to gnupg 2

K

key management 3
key ring, browsing 3
key server, querying 8

L

loopback pinentry 10

M

mail-mode integration 5
multiple file operations 5

P

passphrases, entering and caching 11
pinentry provided by gnupg 10
pinentry, emacs as 10
private key ring, browsing 3
public key encryption, passphrase entry for 6

Q

query key server 8

R

region operations, cryptographic 4
reporting bugs 12

S

sending signed/encrypted mails 5
sign file 5
sign region 4
symmetric encryption, passphrase entry for 6

T

temporary files created by easypg assistant 6

V

verify file 5
verify region 4
version compatibility with gnupg 9

Key Index

:		C
		C-c C-e C-d..... 5
		C-c C-e C-e..... 6
: d.....	5	C-c C-e C-s..... 6
: e.....	5	C-c C-e C-v..... 6
: s.....	5	C-c C-e d..... 5
: v.....	5	C-c C-e e..... 6
		C-c C-e s..... 6
		C-c C-e v..... 6

Function Index

epa-decrypt-armor-in-region	4	epa-import-keys	3
epa-decrypt-file	5	epa-import-keys-region	4
epa-decrypt-region	4	epa-insert-keys	3
epa-delete-keys	4	epa-list-keys	3
epa-dired-do-decrypt	5	epa-list-secret-keys	3
epa-dired-do-encrypt	5	epa-mail-decrypt	5
epa-dired-do-sign	5	epa-mail-encrypt	6
epa-dired-do-verify	5	epa-mail-sign	6
epa-encrypt-file	5	epa-mail-verify	6
epa-encrypt-region	4	epa-sign-file	5
epa-file-disable	7	epa-sign-region	4
epa-file-enable	7	epa-verify-cleartext-in-region	4
epa-file-select-keys	7	epa-verify-file	5
epa-import-armor-in-region	4	epa-verify-region	4

Variable Index

A

allow-loopback-pinentry 10

E

epa-file-cache-passphrase-for-symmetric-
 encryption 7

epa-file-encrypt-to 7

epa-file-inhibit-auto-save 8

epa-file-name-regexp 7

epa-file-select-keys 7

epa-keys-select-method 4

epa-mail-aliases 6

epg-pinentry-mode 10