PGG

by Daiki Ueno

This file describes PGG, an Emacs interface to various PGP implementations.

PGG

これは PGG のマニュアルです。PGG は、安全な通信のための様々なツールと Emacs の仲を取り持つライブラリーです。また、PGG は MIME メッセージの暗号化と解読、それに署名と検証のための単純なユーザーインタフェースも提供します。

1 概要

PGG は、安全な通信のための様々なツールと Emacs の仲を取り持つライブラリーです。同様の機能は Mailcrypt も持っていますが、Mailcrypt は PGP/MIME のインフラで通常用いられる分離された PGP メッセージを取り扱うことができません。これが、私 (作者) が新しいライブラリーを書いた主な理由です。

PGP/MIME は MIME Object Security Services (RFC1848) の実装です。その標準は RFC2015 で記述されています。

2 必要条件

PGG を使うためには、少なくとも一つのプライバシー保護システムの実装が必要です。このマニュアルは、そのようなプログラムをすでに取得、インストールしていて、基本的な使い方を知っていることを想定しています。

ディフォルトでは PGG は GnuPG を使います。そのようなシステムに慣れていないのであれば、`http://www.gnupg.org/documentation/` にある GNU Privacy Handbook (GPH) に目を通すことを勧めます。

GnuPG を使う場合には `gpg-agent` の利用を推奨します。それはバージョン 2.0 以降の GnuPG とともに配布されています。これは、どんなプロトコルを使うかとは無関係に秘密鍵を管理するデーモンで、パスフレーズを入力してキャッシュするための最も安全な手段を提供します (see Section 3.3 [Caching passphrase], page 5)。それが稼働している場合、PGG はディフォルトで `gpg-agent` を使おうとします。See section “Invoking GPG-AGENT” in *Using the GNU Privacy Guard*.

PGG は Pretty Good Privacy バージョン 2 またはバージョン 5 もサポートします。

3 使い方

このライブラリーの最上位インタフェースはとても単純で、公開鍵による暗号の操作のみを想定しています。

PGG を使うためには、アプリケーションプログラムの冒頭で次の S 式を評価して下さい。

```
(require 'pgg)
```

実行時に pgg.el の存在を確認したいなら、上記の方法ではなく以下のように、必要な機能の autoload を設定することもできます。

```
(autoload 'pgg-encrypt-region "pgg"
  "Encrypt the current region." t)
(autoload 'pgg-encrypt-symmetric-region "pgg"
  "Encrypt the current region with symmetric algorithm." t)
(autoload 'pgg-decrypt-region "pgg"
  "Decrypt the current region." t)
(autoload 'pgg-sign-region "pgg"
  "Sign the current region." t)
(autoload 'pgg-verify-region "pgg"
  "Verify the current region." t)
(autoload 'pgg-insert-key "pgg"
  "Insert the ASCII armored public key." t)
(autoload 'pgg-snarf-keys-region "pgg"
  "Import public keys in the current region." t)
```

3.1 ユーザーコマンド

この時点で、いくつかの暗号に関するコマンドを使うことができます。これらのコマンドの挙動は起動方法に依存します。これらのコマンドは、ライブラリー関数として利用されることもあるからです。例えば、あなたがある署名者の公開鍵を持っていないと `pgg-verify-region` という関数は即座に失敗しますが、これが対話的に呼び出された場合には、サーバーから公開鍵をダウンロードするかどうかをあなたに尋ねます。

`pgg-encrypt-region` *start end recipients* **&optional** *sign passphrase* [Command]

start と *end* の間の領域を *recipients* 宛に送るものとして暗号化します。対話的に呼ぶと、受信者を尋ねます。

暗号化に成功すると、現在の領域の内容を暗号化したデータで置き換えます。

オプション引数 *sign* が `nil` でなかったら、署名と暗号化を同時に行ないます。現在この機能は GnuPG で動作することが確認されていますが、PGP や PGP5 では動作しないかもしれません。

オプション引数 *passphrase* が `nil` だったら、パスフレーズのキャッシュからか、またはユーザーに入力してもらうことによってパスフレーズを得ます。

`pgg-encrypt-symmetric-region` **&optional** *start end passphrase* [Command]

現在の *start* と *end* の間の領域を、共通鍵暗号 (symmetric cipher) で暗号化します。呼び出した後でパスフレーズが尋ねられます。

オプション引数 *passphrase* が `nil` だったら、パスフレーズのキャッシュからか、またはユーザーに入力してもらうことによってパスフレーズを得ます。

共通鍵暗号による暗号化は、現在 GnuPG だけで実装されています。

`pgg-decrypt-region` *start end* **&optional** *passphrase* [Command]
start と *end* の間の領域を解読します。解読に成功すると、現在の領域の内容を解読したデータで置き換えます。

オプション引数 *passphrase* が `nil` だったら、パスフレーズのキャッシュからか、またはユーザーに入力してもらうことによってパスフレーズを得ます。

`pgg-sign-region` *start end* **&optional** *cleartext passphrase* [Command]
start と *end* の間のテキストに署名します。三番目のオプション引数 *cleartext* が `nil` ではないか、あるいは対話的に呼ばれた場合、分離された署名を作りません。そのような場合には、現在の領域の内容を署名したデータで置き換えます。

オプション引数 *passphrase* が `nil` だったら、パスフレーズのキャッシュからか、またはユーザーに入力してもらうことによってパスフレーズを得ます。

`pgg-verify-region` *start end* **&optional** *signature fetch* [Command]
start と *end* の間の領域にある署名を検証します。三番目のオプション引数 *signature* が `nil` でなかったら、その引数は現在の領域の分離された署名のファイルとして取り扱われます。

四番目のオプション引数 *fetch* が `nil` ではないか、あるいは対話的に呼ばれた場合、公開鍵をサーバーから取得します。

`pgg-insert-key` [Command]
ユーザーの公開鍵を取得して、それを ASCII 装甲の形式で挿入します。

`pgg-snarf-keys-region` *start end* [Command]
start と *end* の間の領域にある公開鍵を集め、ユーザーの鍵束 (keyring) に追加します。

3.2 どの実装を使うか

PGP は歴史が長く、今では多くの実装を利用することができるので、それぞれが持っている個々の機能がずいぶん異なっていることがあります。例えば GnuPG を使っているのならば、暗号アルゴリズムとして 3DES や CAST5、BLOWFISH などを選ぶことができますが、PGP のバージョン 2 は IDEA しかサポートしていません。

どの実装を使うかは `pgg-scheme` 変数が制御します。`nil` だったら (それがディフォルト)、代わりに `pgg-default-scheme` 変数の値を使います。

`pgg-scheme` [Variable]
どの PGP 実装を用いるかを強制します。設定できるのは `gpg`、`pgp` および `pgp5` のどれかです。ディフォルトは `nil` です。

`pgg-default-scheme` [Variable]
ディフォルトの PGP 実装です。値は `gpg`、`pgp` および `pgp5` のどれかでなければなりません。ディフォルトは `gpg` です。

3.3 パスフレーズをキャッシュする

PGP 実装として GnuPG (gpg) を使うのであれば、パスフレーズの入力とキャッシュ[1] するために `gpg-agent` というプログラムを使うことを推奨します。

[1] `gpg-agent` は実際にはパスフレーズではなくて秘密鍵をキャッシュします。一方ユーザーの視点からは、この技術的な差異は見えません。

`pgg-gpg-use-agent` [Variable]
: `nil` でない値では、可能な場合は常にいつでも `gpg-agent` を使おうとします。ディフィフォルトは `t` です。`gpg-agent` が稼働していないか、または GnuPG が現在の PGP 実装として選択されていない場合は、PGG 自身が持っているパスフレーズをキャッシュする仕組みが使われます (下記参照)。

PGG で `gpg-agent`を使うには、第一に `gpg-agent` が確実に稼働しているようにして下さい。例えば X Window System を走らせているのであれば、以下の行をあなたの '`.xsession`' ファイルに置くことによって、それを確実にすることができます:

```
eval "$(gpg-agent --daemon)"
```

`gpg-agent` の起動に関するさらに詳しいことは、See section "Invoking GPG-AGENT" in *Using the GNU Privacy Guard*.

GnuPG のパスフレーズを必要とする PGG の機能を実行するときはいつも、GnuPG は `gpg-agent` とやり取りを行ない、それはあなたにパスフレーズを入力することを要求します。しかし `gpg-agent` がその結果を「キャッシュ」するので、次回以降の実行では再びパスフレーズの入力は要りません。(通常このキャッシュは一定時間経過後に期限切れ消去されます。これを変更するには、`gpg-agent` を起動するときに `--default-cache-ttl` オプションを使って下さい。)

X Window System の環境では `gpg-agent` はパスフレーズの入力を要求するためにグラフィックなウィンドウを開きます。しかし文字端末で Emacs を使っている場合は、`gpg-agent` は端末からの入力を受け取る上で問題があります。それが Emacs に送られてしまうからです。この問題に対処するための暫定的な対策のひとつは、`gpg-agent` を `--keep-tty` オプションとともに Emacs とは別の端末で走らせることです。これは `gpg-agent` に、パスフレーズの入力にそれ自身の端末を使うようにさせます。

`gpg-agent` を使わない場合、PGG は Emacs を介してパスフレーズの入力を要求します。これにはパスフレーズをキャッシュする仕組みがあり、それは変数 `pgg-cache-passphrase` で制御されます (下記参照)。

`gpg-agent` ではなく PGG でパスフレーズを扱う場合には安全上のリスクがあります。Emacs の要求に従ってパスフレーズを入力すると、それは一時的に Emacs が実行しているメモリーに cleartext 文字列として格納されます。もしそのメモリーがディスクとの間で swap されると、理論上 root ユーザーはパスフレーズを swap ファイルから抽出することができます。その上、そのシステムが廃棄されたり盗難に会った後も、その cleartext のパスフレーズが含まれている swap ファイルはディスクに残っているかもしれないのです。`gpg-agent` はメモリーを lock するような策をもって、この問題を回避しています。それは Emacs には実装されていません。

`pgg-cache-passphrase` [Variable]
: `nil` でなければ、パスフレーズを保持します。初期値は `t` です。しかし、あなたがセキュリティについて気掛かりなら、この変数を `nil` に設定することによって、パスフレーズのキャッシュをやめさせることができます。

`pgg-passphrase-cache-expiry` [Variable]
: パスフレーズを保持しておく時間を秒で指定します。

パスフレーズが非-ASCII 文字を含んでいる場合は、それをエンコードするための coding system を指定する必要があります。GnuPG はパスフレーズを文字列としてではなく、バイト列として扱うからです。

`pgg-passphrase-coding-system` [Variable]
: パスフレーズをエンコードするための coding system です。

3.4 ディフォルトのユーザー ID

通常 PGP の実装は、暗号化および復号化に使う適切な鍵を選ぶことができますが、あなたが一つ以上の鍵を持っている場合、用いる鍵の id を指定する必要があります。

`pgg-default-user-id` [Variable]
ディフォルトのユーザー ID です。指定しない場合は '`(user-login-name)`' の戻り値がディフォルトになります。この変数はカスタマイズ可能です。

`pgg-gpg-user-id` [Variable]
GnuPG で使うディフォルトのユーザー ID です。ディフォルトは '`nil`' です。`nil` ではない値にすると、'`pgg-default-user-id`' より優先して使われます。カスタマイズ可能です。

`pgg-pgp-user-id` [Variable]
PGP 2.x/6.x で使うディフォルトのユーザー ID です。ディフォルトは '`nil`' です。`nil` ではない値にすると、'`pgg-default-user-id`' より優先して使われます。カスタマイズ可能です。

`pgg-pgp5-user-id` [Variable]
PGP 5.x で使うディフォルトのユーザ ID です。ディフォルトは '`nil`' です。`nil` ではない値にすると、'`pgg-default-user-id`' より優先して使われます。カスタマイズ可能です。

4 構成

PGG は「PGP 実装のスキーム (枠組)」という考えを導入します。以後、「スキーム (scheme)」と表記します。この用語は luna object system での singleton object に由来します。

PGG は PGP の機能にアクセスすると同時にそれを開発するために設計されたので、その構成は、相互運用性だけでなく拡張性も考慮する必要がありました。この章では、PGG のバックエンドをどのように記述するかを探しながら、PGG がどのようにつくられているかを探検してみましょう。

4.1 初期化

スキームは、使う前に初期化されなければなりません。ただ一つのスキームを使うことを保証するのが良いでしょう。

以下のコードは 'pgg-gpg.el' からの抜き書きです。ある pgg-gpg のスキームがいったん初期化されると、それは pgg-scheme-gpg-instance 変数に保存され、以後、再利用されます。

```
(defvar pgg-scheme-gpg-instance nil)

(defun pgg-make-scheme-gpg ()
  (or pgg-scheme-gpg-instance
      (setq pgg-scheme-gpg-instance
    (luna-make-entity 'pgg-scheme-gpg))))
```

関数の名前は pgg-make-scheme- の後ろにバックエンド名を付加したものにしなければなりません。

4.2 バックエンドのメソッド

各バックエンドには、これらのメソッドが存在しなければなりません。メソッドの実行結果のステータスを知らせなければならないので、メソッドの出力は特別なバッファーに保存されます (see Section 4.3 [Getting output], page 9)。

`pgg-scheme-lookup-key` *scheme string* **&optional** *type* [Method]
: *string* に関連付けられた鍵を返します。三番目のオプション引数 *type* が非-nil だったら、秘密の鍵束から検索します。

`pgg-scheme-encrypt-region` *scheme start end recipients* **&optional** *sign passphrase* [Method]
: *start* と *end* の間の領域を *recipients* 宛に送るものとして暗号化します。オプション引数 *sign* が nil でなかったら、署名と暗号化を同時に行ないます。暗号化に成功すると t を、失敗すると nil を返します。

`pgg-scheme-encrypt-symmetric-region` *scheme start end* **&optional** *passphrase* [Method]
: 現在の *start* と *end* の間の領域を、共通鍵暗号 (symmetric cipher) とパスフレーズで暗号化します。暗号化に成功すると t を返し、そうでなければ nil を返します。この機能は現在 GnuPG だけで実装されています。

`pgg-scheme-decrypt-region` *scheme start end* **&optional** *passphrase* [Method]
: *start* と *end* の間の領域を解読します。解読に成功すると t を、失敗すると nil を返します。

`pgg-scheme-sign-region` *scheme start end* **&optional** *cleartext passphrase* [Method]
start と *end* の間のテキストに署名します。三番目のオプション引数 *cleartext* が `nil` ではない場合、分離された署名を作りません。署名に成功すると `t` を、失敗すると `nil` を返します。

`pgg-scheme-verify-region` *scheme start end* **&optional** *signature* [Method]
start と *end* の間の領域にある署名を検証します。三番目のオプション引数 *signature* が `nil` でなかったら、その引数は現在の領域の分離された署名のファイルとして取り扱われます。署名が正しく検証された場合は `t` を、失敗すると `nil` を返します。

`pgg-scheme-insert-key` *scheme* [Method]
ユーザーの公開鍵を取得して、それを ASCII 装甲の形式で挿入します。成功すると `t` を、失敗すると `nil` を返します。

`pgg-scheme-snarf-keys-region` *scheme start end* [Method]
start と *end* の間の領域にある公開鍵を集め、ユーザーの鍵束 (keyring) に追加します。成功すると `t` を、失敗すると `nil` を返します。

4.3 出力を得る

バックエンド メソッド (see Section 4.2 [Back end methods], page 8) の出力は特別なバッファーに格納されます。したがって、これらのメソッドは実行結果を伝える必要があります。

`pgg-errors-buffer` [Variable]
PGP コマンド実行時の標準エラー出力は、このバッファーに格納されます。

`pgg-output-buffer` [Variable]
PGP コマンド実行時の標準出力は、このバッファーに格納されます。

`pgg-status-buffer` [Variable]
PGP コマンド実行時のその他の結果の情報は、このバッファーに格納されます。

5 OpenPGP パケットの解析

OpenPGP のメッセージのフォーマットは、相互運用できるアプリケーション開発に必要なすべての情報を出力するように維持されています。その標準は RFC2440 に記載されています。

PGG は OpenPGP パケットに対応した独自のメッセージ解析を行ないます。

`pgg-parse-armor` *string* [Function]
string 内のパケットの並びを `list` の形式で返します。

`pgg-parse-armor-region` *start end* [Function]
start と *end* の間の領域にあるパケットの並びを `list` の形式で返します。

`pgg-ignore-packet-checksum` [Variable]
`nil` でなかったら、パケットのチェックサムを検証しません。

6 GNU フリー文書利用許諾契約書

訳注: 非公式な日本語訳 (http://www.opensource.jp/fdl/fdl.ja.html.euc-jp) があります。

Appendix A GNU Free Documentation License

Version 1.2, November 2002

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. Secondarily, 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.

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 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.

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 1.2
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.

Function Index

Variable Index

Short Contents

Table of Contents