PGG

by Daiki Ueno

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

PGG

This manual describes PGG. PGG is an interface library between Emacs and various tools for secure communication. PGG also provides a simple user interface to encrypt, decrypt, sign, and verify MIME messages.

1 Overview

PGG is an interface library between Emacs and various tools for secure communication. Even though Mailcrypt has similar feature, it does not deal with detached PGP messages, normally used in PGP/MIME infrastructure. This was the main reason why I wrote the new library.

PGP/MIME is an application of MIME Object Security Services (RFC1848). The standard is documented in RFC2015.

2 Prerequisites

PGG requires at least one implementation of privacy guard system. This document assumes that you have already obtained and installed them and that you are familiar with its basic functions.

By default, PGG uses GnuPG. If you are new to such a system, I recommend that you should look over the GNU Privacy Handbook (GPH) which is available at `http://www.gnupg.org/documentation/`.

When using GnuPG, we recommend the use of the `gpg-agent` program, which is distributed with versions 2.0 and later of GnuPG. This is a daemon to manage private keys independently from any protocol, and provides the most secure way to input and cache your passphrases (see Section 3.3 [Caching passphrase], page 6). By default, PGG will attempt to use `gpg-agent` if it is running. See section "Invoking GPG-AGENT" in *Using the GNU Privacy Guard*.

PGG also supports Pretty Good Privacy version 2 or version 5.

3 How to use

The toplevel interface of this library is quite simple, and only intended to use with public-key cryptographic operation.

To use PGG, evaluate following expression at the beginning of your application program.

```
(require 'pgg)
```

If you want to check existence of pgg.el at runtime, instead you can list autoload setting for desired functions as follows.

```
(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 User Commands

At this time you can use some cryptographic commands. The behavior of these commands relies on a fashion of invocation because they are also intended to be used as library functions. In case you don't have the signer's public key, for example, the function `pgg-verify-region` fails immediately, but if the function had been called interactively, it would ask you to retrieve the signer's public key from the server.

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

Encrypt the current region between *start* and *end* for *recipients*. When the function were called interactively, you would be asked about the recipients.

If encryption is successful, it replaces the current region contents (in the accessible portion) with the resulting data.

If optional argument *sign* is non-`nil`, the function is request to do a combined sign and encrypt. This currently is confirmed to work with GnuPG, but might not work with PGP or PGP5.

If optional *passphrase* is `nil`, the passphrase will be obtained from the passphrase cache or user.

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

Encrypt the current region between *start* and *end* using a symmetric cipher. After invocation you are asked for a passphrase.

If optional *passphrase* is `nil`, the passphrase will be obtained from the passphrase cache or user.

symmetric-cipher encryption is currently only implemented for GnuPG.

`pgg-decrypt-region` *start end* **&optional** *passphrase* [Command]
Decrypt the current region between *start* and *end*. If decryption is successful, it replaces the current region contents (in the accessible portion) with the resulting data.

If optional *passphrase* is `nil`, the passphrase will be obtained from the passphrase cache or user.

`pgg-sign-region` *start end* **&optional** *cleartext passphrase* [Command]
Make the signature from text between *start* and *end*. If the optional third argument *cleartext* is non-`nil`, or the function is called interactively, it does not create a detached signature. In such a case, it replaces the current region contents (in the accessible portion) with the resulting data.

If optional *passphrase* is `nil`, the passphrase will be obtained from the passphrase cache or user.

`pgg-verify-region` *start end* **&optional** *signature fetch* [Command]
Verify the current region between *start* and *end*. If the optional third argument *signature* is non-`nil`, it is treated as the detached signature file of the current region.

If the optional 4th argument *fetch* is non-`nil`, or the function is called interactively, we attempt to fetch the signer's public key from the key server.

`pgg-insert-key` [Command]
Retrieve the user's public key and insert it as ASCII-armored format.

`pgg-snarf-keys-region` *start end* [Command]
Collect public keys in the current region between *start* and *end*, and add them into the user's keyring.

3.2 Selecting an implementation

Since PGP has a long history and there are a number of PGP implementations available today, the function which each one has differs considerably. For example, if you are using GnuPG, you know you can select cipher algorithm from 3DES, CAST5, BLOWFISH, and so on, but on the other hand the version 2 of PGP only supports IDEA.

Which implementation is used is controlled by the `pgg-scheme` variable. If it is `nil` (the default), the value of the `pgg-default-scheme` variable will be used instead.

`pgg-scheme` [Variable]
Force specify the scheme of PGP implementation. The value can be set to `gpg`, `pgp`, and `pgp5`. The default is `nil`.

`pgg-default-scheme` [Variable]
The default scheme of PGP implementation. The value should be one of `gpg`, `pgp`, and `pgp5`. The default is `gpg`.

3.3 Caching passphrase

When using GnuPG (gpg) as the PGP scheme, we recommend using a program called `gpg-agent` for entering and caching passphrases[1].

`pgg-gpg-use-agent` [Variable]

If non-`nil`, attempt to use `gpg-agent` whenever possible. The default is `t`. If `gpg-agent` is not running, or GnuPG is not the current PGP scheme, PGG's own passphrase-caching mechanism is used (see below).

To use `gpg-agent` with PGG, you must first ensure that `gpg-agent` is running. For example, if you are running in the X Window System, you can do this by putting the following line in your '`.xsession`' file:

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

For more details on invoking `gpg-agent`, See section "Invoking GPG-AGENT" in *Using the GNU Privacy Guard*.

Whenever you perform a PGG operation that requires a GnuPG passphrase, GnuPG will contact `gpg-agent`, which prompts you for the passphrase. Furthermore, `gpg-agent` "caches" the result, so that subsequent uses will not require you to enter the passphrase again. (This cache usually expires after a certain time has passed; you can change this using the `--default-cache-ttl` option when invoking `gpg-agent`.)

If you are running in a X Window System environment, `gpg-agent` prompts for a passphrase by opening a graphical window. However, if you are running Emacs on a text terminal, `gpg-agent` has trouble receiving input from the terminal, since it is being sent to Emacs. One workaround for this problem is to run `gpg-agent` on a different terminal from Emacs, with the `--keep-tty` option; this tells `gpg-agent` use its own terminal to prompt for passphrases.

When `gpg-agent` is not being used, PGG prompts for a passphrase through Emacs. It also has its own passphrase caching mechanism, which is controlled by the variable `pgg-cache-passphrase` (see below).

There is a security risk in handling passphrases through PGG rather than `gpg-agent`. When you enter your passphrase into an Emacs prompt, it is temporarily stored as a cleartext string in the memory of the Emacs executable. If the executable memory is swapped to disk, the root user can, in theory, extract the passphrase from the swapfile. Furthermore, the swapfile containing the cleartext passphrase might remain on the disk after the system is discarded or stolen. `gpg-agent` avoids this problem by using certain tricks, such as memory locking, which have not been implemented in Emacs.

`pgg-cache-passphrase` [Variable]

If non-`nil`, store passphrases. The default value of this variable is `t`. If you are worried about security issues, however, you could stop the caching of passphrases by setting this variable to `nil`.

`pgg-passphrase-cache-expiry` [Variable]

Elapsed time for expiration in seconds.

[1] Actually, `gpg-agent` does not cache passphrases but private keys. On the other hand, from a user's point of view, this technical difference isn't visible.

If your passphrase contains non-ASCII characters, you might need to specify the coding system to be used to encode your passphrases, since GnuPG treats them as a byte sequence, not as a character sequence.

`pgg-passphrase-coding-system` [Variable]
Coding system used to encode passphrase.

3.4 Default user identity

The PGP implementation is usually able to select the proper key to use for signing and decryption, but if you have more than one key, you may need to specify the key id to use.

`pgg-default-user-id` [Variable]
User ID of your default identity. It defaults to the value returned by '`(user-login-name)`'. You can customize this variable.

`pgg-gpg-user-id` [Variable]
User ID of the GnuPG default identity. It defaults to '`nil`'. This overrides '`pgg-default-user-id`'. You can customize this variable.

`pgg-pgp-user-id` [Variable]
User ID of the PGP 2.x/6.x default identity. It defaults to '`nil`'. This overrides '`pgg-default-user-id`'. You can customize this variable.

`pgg-pgp5-user-id` [Variable]
User ID of the PGP 5.x default identity. It defaults to '`nil`'. This overrides '`pgg-default-user-id`'. You can customize this variable.

4 Architecture

PGG introduces the notion of a "scheme of PGP implementation" (used interchangeably with "scheme" in this document). This term refers to a singleton object wrapped with the luna object system.

Since PGG was designed for accessing and developing PGP functionality, the architecture had to be designed not just for interoperability but also for extensiblity. In this chapter we explore the architecture while finding out how to write the PGG backend.

4.1 Initializing

A scheme must be initialized before it is used. It had better guarantee to keep only one instance of a scheme.

The following code is snipped out of '`pgg-gpg.el`'. Once an instance of `pgg-gpg` scheme is initialized, it's stored to the variable `pgg-scheme-gpg-instance` and will be reused from now on.

```
(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))))
```

The name of the function must follow the regulation—`pgg-make-scheme-` follows the backend name.

4.2 Backend methods

In each backend, these methods must be present. The output of these methods is stored in special buffers (Section 4.3 [Getting output], page 9), so that these methods must tell the status of the execution.

`pgg-scheme-lookup-key` *scheme string* **&optional** *type* [Method]
: Return keys associated with *string*. If the optional third argument *type* is non-`nil`, it searches from the secret keyrings.

`pgg-scheme-encrypt-region` *scheme start end recipients* **&optional** *sign passphrase* [Method]
: Encrypt the current region between *start* and *end* for *recipients*. If *sign* is non-`nil`, do a combined sign and encrypt. If encryption is successful, it returns `t`, otherwise `nil`.

`pgg-scheme-encrypt-symmetric-region` *scheme start end* **&optional** *passphrase* [Method]
: Encrypt the current region between *start* and *end* using a symmetric cipher and a passphrases. If encryption is successful, it returns `t`, otherwise `nil`. This function is currently only implemented for GnuPG.

`pgg-scheme-decrypt-region` *scheme start end* **&optional** *passphrase* [Method]
Decrypt the current region between *start* and *end*. If decryption is successful, it returns `t`, otherwise `nil`.

`pgg-scheme-sign-region` *scheme start end* **&optional** *cleartext* *passphrase* [Method]
Make the signature from text between *start* and *end*. If the optional third argument *cleartext* is non-`nil`, it does not create a detached signature. If signing is successful, it returns `t`, otherwise `nil`.

`pgg-scheme-verify-region` *scheme start end* **&optional** *signature* [Method]
Verify the current region between *start* and *end*. If the optional third argument *signature* is non-`nil`, it is treated as the detached signature of the current region. If the signature is successfully verified, it returns `t`, otherwise `nil`.

`pgg-scheme-insert-key` *scheme* [Method]
Retrieve the user's public key and insert it as ASCII-armored format. On success, it returns `t`, otherwise `nil`.

`pgg-scheme-snarf-keys-region` *scheme start end* [Method]
Collect public keys in the current region between *start* and *end*, and add them into the user's keyring. On success, it returns `t`, otherwise `nil`.

4.3 Getting output

The output of the backend methods (Section 4.2 [Backend methods], page 8) is stored in special buffers, so that these methods must tell the status of the execution.

`pgg-errors-buffer` [Variable]
The standard error output of the execution of the PGP command is stored here.

`pgg-output-buffer` [Variable]
The standard output of the execution of the PGP command is stored here.

`pgg-status-buffer` [Variable]
The rest of status information of the execution of the PGP command is stored here.

5 Parsing OpenPGP packets

The format of OpenPGP messages is maintained in order to publish all necessary information needed to develop interoperable applications. The standard is documented in RFC 2440.

PGG has its own parser for the OpenPGP packets.

`pgg-parse-armor` *string* [Function]
List the sequence of packets in *string*.

`pgg-parse-armor-region` *start end* [Function]
List the sequence of packets in the current region between *start* and *end*.

`pgg-ignore-packet-checksum` [Variable]
If non-`nil`, don't check the checksum of the packets.

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