Substituir PGP 2.x por GnuPG

Este documento está basado en una guía de compatibilidad PGP 2.x/GnuPG (http://www.toehold.com/~kyle/pgp-compat.html) anterior, desarrollada por Kyle Hasselbacher (<`kyle@toehold.com`>). La guía fue reeditada y ampliada por Mike Ashley (<`jashley@acm.org`>). Michael Fischer v. Mollard (<`mfvm@gmx.de`>) transformó el código HTML a DocBook SGML, y también añadió algunos datos. Algunos de los temas aquí tratados tienen su origen en las listas de correo de `gnupg-devel` y `gnupg-user`. La solución dada al problema de firmar y cifrar a un tiempo con una clave RSA fue tomada del guión de compatibilidad (http://muppet.faveve.uni-stuttgart.de/~gero/gpg-2comp/changes.html) de Gero Treuner. Para cualquier duda, error, o sugerencia sobre este manual, diríjase al mantenedor de este documento, Mike Ashley (<`jashley@acm.org`>). Para cualquier duda, corrección, o sugerencia sobre la versión en castellano, diríjase al traductor, Horacio (<`homega@ciberia.es`>).

Introducción

Este documento describe cómo comunicarse con otras personas que todavía estén usando viejas versiones de PGP 2.x. GnuPG puede usarse como un substituto completo de PGP 2.x. Con GnuPG es posible cifrar y descifrar mensajes PGP 2.x, importando primero las claves viejas, pero no se pueden generar claves de PGP 2.x. En este documento se demuestra cómo ampliar la distribución normal de GnuPG para que funcione con claves PGP 2.x, y muestra qué opciones deben ser usadas para asegurar la interoperabilidad con los usuarios de PGP 2.x. También se avisa de anomalías en la interoperabilidad entre PGP 2.x y GnuPG.

Nota: El uso de los módulos de extensión `idea.c` y `rsa.c` sin las correspondientes licencias de estos algoritmos puede ser ilegal. En este documento no se recomienda que se usen dichos módulos. Si Vd. dispone de claves PGP 2.x, el autor sugiere que las revoque en favor de otras nuevas y que anime a las personas con las que mantenga correspondencia y que continúen usando claves PGP 2.x, a que hagan lo mismo.

Ampliar GnuPG para su funcionamiento con claves PGP 2.x

La distribución normal de GnuPG no funciona con claves PGP 2.x debido a que PGP 2.x hace uso de IDEA como algoritmo de cifrado simétrico, y de RSA como algoritmo de clave pública. Estos dos algoritmos están patentados[1]y sólo pueden ser usados bajo ciertas condiciones restrictivas. La política de GNU es la de no hacer uso de algoritmos patentados, dado que éstas son una contradicción con el espíritu del "software"libre. La utilización de estos algoritmos representa una barrera para el uso libre de GnuPG.

El uso de RSA e IDEA sin una licencia sobre éstos puede ser o no legal dependiendo de varias cuestiones. RSA sólo está patentado en los Estados Unidos, por lo tanto sí que es lícito desarrollar versiones de RSA

[1] La patente de RSA finaliza en Septiembre de 2000. La patente de IDEA finaliza en el año 2011.

fuera de los EE.UU. El módulo de extensión de RSA para GnuPG es una de estas versiones, y en consecuencia sí que puede ser usado legalmente fuera de los Estados Unidos, aunque sería ilegal si lo usara dentro de este país. En los Estados Unidos existe una implementación de referencia para RSA, llamada RSAREF, y que se encuentra disponible por ftp en funet.fi (ftp://ftp.funet.fi/pub/crypt/cryptography/asymmetric/rsa/rsaref2.tar.gz), o en debian.org (ftp://non-us.debian.org/debian-non-US/dists/stable/non-US/source/rsaref_19930105.orig.tar.gz), y que puede usarse legalmente en los EE.UU. sin cargo alguno para el uso con fines no lucrativos. Debido a leyes que restringen la exportación de este código de los EE.UU., no puede ser distribuido fuera de este país, y por tanto existen dos modos de integrar RSA en GnuPG: uno para los EE.UU. y Canadá, y otro para el resto del mundo.

La situación de IDEA es más simple. IDEA está patentado en Europa y en los EE.UU., y queda pendiente una patente para Japón. El propietario de la patente, Ascom, concede una licencia (http://www.ascom.ch/infosec/idea/licensing.h con fines no lucrativos gratuita, pero la definición de fines no lucrativos es bastante estricta. Si desea utilizar IDEA para fines comerciales necesita adquirir una licencia.

Para poder usar los módulos de extensión primero hay que obtener el código fuente de éstos, `idea.c` y `rsa.c`, o `rsaref.c`, del directorio de cotribución (ftp://ftp.gnupg.org/pub/gcrypt/contrib/) de código a GnuPG. Una vez se tenga el código, éste debe ser compilado. Si se usa gcc, la compilación será como sigue:

```
alice% gcc -Wall -O2 -shared -fPIC -o idea idea.c
[...]
alice% gcc -Wall -O2 -shared -fPIC -o rsa rsa.c
[...] # ó
alice% gcc -Wall -O2 -shared -fPIC -o rsa rsaref.c /usr/lib/rsaref.a
```

El último argumento `/usr/lib/rsaref.a` se debe substituir con el camino real de la biblioteca RSAREF en el sistema.

Una vez compilado, GnuPG debe recibir las instrucciones para cargarlos. Esto se puede hacer usando la opción `load-extension`, bien desde la línea de órdenes, o bien desde el fichero de opciones, aunque por regla general se hará desde el fichero de opciones. Por ejemplo, si se ha puesto los binarios compilados `idea` y `rsa` en el directorio `~/.gnupg`, en el fichero de opciones se debe añadir

```
load-extension ~/.gnupg/idea
load-extension ~/.gnupg/rsa
```

Si no se especifica un camino de modo explícito, GnuPG busca los módulos de extensión en el directorio de módulos de GnuPG por definición, el cual es `/usr/local/lib/gnupg`. Si se ha compilado GnuPG con prefijo distinto para el directorio de instalación, usando `-prefix PREFIX` durante la configuración del código fuente de GnuPG, entonces el directorio de módulos será `PREFIX/lib/gnupg`. En tal caso, copiar los dos ficheros ‘rsa’ e ‘idea’ en el directorio de módulos descrito arriba. Asegúrese de que estos ficheros tienen los permisos correctos. No es necesario hacer los ficheros ejecutables, ya que estos ficheros no son programas sino módulos compartidos, y por tanto deben tener permiso de lectura para todos.

Importar claves PGP 2.x

Una vez que las extensiones han sido cargadas, el importar un par de claves de PGP 2.x es una tarea fácil usando la opción `import`. Aun así se debe tener cuidado con un par de detalles.

- No se debe exportar una clave privada desde PGP 2.x en forma de fichero en armadura ASCII. Ya que PGP 2.x es anterior a la especificación OpenPGP, la cabecera del mensaje en armadura que usa PGP 2.x no es conforme con OpenPGP. Debido a que la exportación de una clave privada es un caso poco común, GnuPG no comprueba que el fichero en armadura ASCII sea una clave privada.
- GnuPG presupone que las claves públicas importadas van autofirmadas por sus correspondientes claves públicas. Esta es una precaución bastante prudente, y tanto GnuPG como las nuevas versiones de PGP autofirman las claves públicas durante el proceso de su generación. Sin embargo, PGP 2.x no lo hace. Para solventarlo, se puede autofirmar la clave pública antes de exportarla desde PGP 2.x. De modo alternativo, se puede usar la opción `allow-non-selfsigned-uid` para forzar a GnuPG a aceptar la clave. Se recomienda que la clave sea autofirmada antes de ser exportada, o incluso después de haber sido importada usando la opción anterior, ya que el uso de una clave no autofirmada es un riesgo para la seguridad.

```
alice% pgp –kx alice public.pgp
Pretty Good Privacy(tm) 2.6.2 - Public-key encryption for the masses.
[...]
Extracting from key ring: ’/u/alice/.pgp/pubring.pgp’, userid "alice".
Key for user ID: Alice <alice@cyb.org>
1024-bit key, Key ID 24E2C409, created 1999/09/18

Key extracted to file ’public.pgp’.

alice% pgp –kx alice private.pgp .pgp/secring.pgp
Pretty Good Privacy(tm) 2.6.2 - Public-key encryption for the masses.
[...]

Extracting from key ring: ’.pgp/secring.pgp’, userid "alice".
Key for user ID: Alice <alice@cyb.org>
1024-bit key, Key ID 24E2C409, created 1999/09/18

Key extracted to file ’private.pgp’.

alice% gpg –import public.pgp
gpg: key 24E2C409: public key imported
gpg: Total number processed: 1
gpg:               imported: 1  (RSA: 1)

alice%gpg –import private.pgp
gpg: key 24E2C409: secret key imported
gpg: Total number processed: 1
gpg:       secret keys read: 1
gpg:   secret keys imported: 1
```

Usar claves PGP 2.x

Una clave pública importada se puede usar para cifrar documentos para un usuario de PGP 2.x y para verificar firmas que hayan sido generadas con una clave privada PGP 2.x *Es importante comprender que no es posible usar una nueva clave OpenPGP para comunicarse con un usuario PGP 2.x, por tanto es necesario importar una clave vieja PGP 2.x para esta tarea.*

Cifrar un documento para un usuario de PGP 2.x

Para cifrar un documento se usan varias opciones en la línea de órdenes, y el documento que se va a cifrar debe ser especificado como un fichero.

```
alice% gpg –rfc1991 –cipher–algo idea –compress–algo 1 –encrypt –recipient alice secret
gpg:
RSA keys are deprecated; please consider creating a new key and use this key in the future
gpg: this cipher algorithm is depreciated; please use a more standard one!
```

Cada una de las opciones en la línea de órdenes son necesarias.

- La opción `rfc1991` se usa para forzar GnuPG a que sea más conforme con RFC 1991, que es la antigua especificación PGP implementada en PGP 2.x. Si se omite esta opción, la salida de GnuPG estará malformada e inutilizable por PGP 2.x.
- La opción `cipher-algo` especifica el algoritmo de cifrado simétrico con el que el documento será cifrado. En el caso especial de cifrar un documento para una clave pública de PGP 2.x, el algoritmo de cifrado que se especifique debe ser IDEA. Si se omitiera esta opción, el documento se cifrará generalmente con 3DES, un algoritmo que no está implementado en PGP 2.x.
- El algoritmo de compresión indica cómo se formará el resto de la orden. La opción `compress-algo` especifica a GnuPG que debe usar el viejo algoritmo de compresión zlib, que es el usado por PGP 2.x. A pesar de esto, GnuPG usa cabeceras de longitud parcial cuando cifra una cadena de tamaño desconocido, y esto no está implementado en PGP 2.x. El documento que se vaya a cifrar debe estar por lo tanto, en un fichero de modo que GnuPG sepa el tamaño total del documento a cifrar antes de comenzar. Por consiguiente, no es posible usar tuberías al utilizar claves PGP 2.x.

Firmar un documento para un usuario de PGP 2.x

Firmar un documento con una clave vieja no es diferente a hacerlo con una clave nueva.

```
alice% gpg –local–user 0x24E2C409 –sign document
You need a passphrase to unlock the secret key for
user: "Alice <alice@cyb.com>"
1024-bit RSA key, ID 24E2C409, created 1999-09-18

gpg: RSA keys are deprecated; please consider creating a new key and use this
key in the future
```

En este ejemplo, la opción `local-user` se usa para especificar qué clave privada se utilizará para firmar. El fichero de salida es de la forma `document.gpg`. Si la firma va a ser verificada usando PGP 2.x, se debe renombrar a un nombre de fichero con la extensión `.pgp`.

Firmar y cifrar un documento para un usuario de PGP 2.x

GnuPG no posee una implementación nativa para firmar un documento con una clave RSA y al mismo tiempo cifrarlo con una clave RSA. Sin embargo es posible usar una solución que requiere que se lleven a cabo unos cuantos pasos anteriormente. El proceso implica la creación de una firma acompañante y a continuación el uso de ésta para crear un fichero cifrado que pueda ser descifrado y verificado usando PGP 2.x.

Hay cuatro pasos. El primer paso genera una firma acompañante.

```
alice% gpg -detach-signature -recipient alice -local-user 0x24E2C409 document

You need a passphrase to unlock the secret key for
user: "Alice <alice@cyb.com>"
1024-bit RSA key, ID 24E2C409, created 1999-09-18

gpg: RSA keys are deprecated; please consider creating a new key and use this
key in the future
```

El segundo paso convierte el documento a un formato interno, literal, que va descifrado.

```
alice% gpg -store -z 0 -output document.lit document
```

El tercer paso combina la firma acompañante con el documento literal. Es esto lo que PGP 2.x usa para verificar la firma después de descifrarlo.

```
alice% cat Notes.sig Notes.lit | gpg -no-options -no-literal -store -compress-algo 1 -output document.z
gpg: NOTE: -no-literal is not for normal use!
```

El cuarto y último paso implica el uso de GnuPG para descifrar el texto plano y la firma con el objeto de producir un documento firmado y cifrado que pueda ser descifrado y verificado por PGP 2.x.

```
alice% gpg -rfc1991 -cipher-algo idea -no-literal -encrypt -recipient alice -output document.pgp document.z
gpg: NOTE: -no-literal is not for normal use!
gpg: RSA keys are deprecated; please consider creating a new key and use this
key in the future
gpg: this cipher algorithm is depreciated; please use a more standard one!
```

El documento firmado y cifrado también puede ir en armadura ASCII mediante el uso de las opciones de rigor.

```
alice% gpg -rfc1991 -cipher-algo idea -no-literal -encrypt -recipient alice -output document.asc -
armor document.z
gpg: NOTE: -no-literal is not for normal use!
gpg: RSA keys are deprecated; please consider creating a new key and use this
key in the future
gpg: this cipher algorithm is depreciated; please use a more standard one!
```

Descifrar un documento gpg

Una clave privada importada se puede usar para descifrar documentos cifrados para esa clave, así como generar firmas mediante el uso de esa clave. Descifrar un mensaje no es, en este caso, más difícil que cuando se usa cualquier otra clave.

```
alice% gpg secret.pgp

You need a passphrase to unlock the secret key for
user: "Alice <alice@cyb.org>"
1024-bit RSA key, ID 24E2C409, created 1999-09-18

gpg: NOTE: cipher algorithm 1 not found in preferences
gpg: secret.pgp: unknown suffix
Enter new filename [secret]:
```

De nuevo, en este caso, se puede evitar el aviso de error renombrando el fichero de entrada con una extensión `.gpg`. Si se ve un aviso de GnuPG del tipo “cipher algorithm 1 not found in preferences”, se puede ignorar sin problemas.

Verificar una firma de PGP 2.x

Verificar una firma usando generada con una clave PGP 2.x es sencillo.

```
alice% gpg document.pgp
gpg: document.pgp: unknown suffix
Enter new filename [document]:
File ‘document’ exists. Overwrite (y/N)? y
gpg: old style (PGP 2.x) signature
gpg: Signature made Sat Sep 18 17:55:30 1999 EST using RSA key ID 24E2C409
gpg: Good signature from "Alice <alice@cyb.org>"
```

El diálogo para renombrar el fichero puede ser evitado si el documento que se quiere verificar ha sido renombrado con una extensión `.gpg` antes de invocar gpg.

Trabajar con firmas sobre texto

Desde la aparición de la versión 1.0 de GnuPG, existe un problema con el intercambio de documentos con firma sobre el texto entre GnuPG y todas las versiones de PGP. Parece ser que las dificultades se deben a desviaciones en la implementación de la especificación OpenPGP. Respecto a PGP 2.x, las firmas generadas por éste se pueden verificar usando GnuPG, y las firmas generadas con GnuPG se pueden verificar usando PGP 2.x. El documento resultante del proceso de verificación será, en ambos casos, diferente del documento original. Estas diferencias se limitan a espacios en blanco, y por tanto no deberían afectar la legibilidad de los documentos firmados. En caso de que mantener la completa integridad del documento fuera de importancia, se recomienda evitar el uso de firmas sobre texto. En cualquier caso, se insiste una vez más en la recomendación de usar y recomendar el uso, siempre que sea posible, de las nuevas claves OpenPGP generadas por GnuPG.

Apéndice A. GNU Free Documentation License

Version 1.1, March 2000

0. PREAMBLE

The purpose of this License is to make a manual, textbook, or other written document "free"in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or noncommercially. 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 çopyleft", which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

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

1. APPLICABILITY AND DEFINITIONS

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

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

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

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

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

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML designed for human modification. Opaque formats include PostScript, PDF, proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML produced by some word processors for output purposes only.

The "Title Page"means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, "Title Page"means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.

2. VERBATIM COPYING

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

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

3. COPYING IN QUANTITY

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

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

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

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

4. MODIFICATIONS

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

A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.
B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has less than five).
C. State on the Title page the name of the publisher of the Modified Version, as the publisher.
D. Preserve all the copyright notices of the Document.
E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.
F. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.
G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.
H. Include an unaltered copy of this License.
I. Preserve the section entitled "History", and its title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.
J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.
K. In any section entitled "Acknowledgements" or "Dedications", preserve the section's title, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.

L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.
M. Delete any section entitled "Endorsements". Such a section may not be included in the Modified Version.
N. Do not retitle any existing section as "Endorsements" or to conflict in title with any Invariant Section.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.

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

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

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

5. COMBINING DOCUMENTS

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

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

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

6. COLLECTIONS OF DOCUMENTS

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

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

7. AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, does not as a whole count as a Modified Version of the Document, provided no compilation copyright is claimed for the compilation. Such a compilation is called an .ªggregate", and this License does not apply to the other self-contained works thus compiled with the Document, on account of their being thus compiled, if they are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one quarter of the entire aggregate, the Document's Cover Texts may be placed on covers that surround only the Document within the aggregate. Otherwise they must appear on covers around the whole aggregate.

8. TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires 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 provided that you also include the original English version of this License. In case of a disagreement between the translation and the original English version of this License, the original English version will prevail.

9. TERMINATION

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

10. FUTURE REVISIONS OF THIS LICENSE

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

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

How to use this License for your documents

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

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

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

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