PGP 6.5.1
Platform-Independent Source Code

Volume 1 of 18

Edited by Philip R. Zimmermann

July 31, 1999

A printed book or other printed material setting forth encryption source code is not itself subject to the EAR (see Sec. 734.3(b)(2)). Bureau of Export Administration, Commerce Interim Rule of December 30, 1996

ISBN 1-58368-015-2

7-99. Printed in the United States of America.

Copies of this publication can be obtained by contacting:

Printers Inc. Bookstore
310 California Avenue
Palo Alto, CA 94306
(650) 327–6500
(800) 742–0402
pibooks@pibooks.com
http://www.pibooks.com

Information on available books can be obtained by contacting:

Network Associates, Inc.
PGP Publication Group
3965 Freedom Circle
Santa Clara, CA 95054
(408) 346–3440
info@pgp.com
http://www.pgp.com

ISBN 1-58368-015-2

The source code and other tools contained in this eight-volume set are the foundation needed to build PGP 65.1 on all platforms. In order to build PGP 6.5.1 for a particualr platofrm, you will need the platform-specific source code set in addition to this one.

About These Books

These books contain the source code and other tools that make up a software package called Pretty Good Privacy, or PGP, Version 6.5.1. The code is divided into two parts, the PGP application clients, and the PGPsdk software developer's kit, the portable library which they are based on.

PGP is a high security cryptographic software application for Windows™ and Macintosh™ platforms. Since its initial release by Philip Zimmermann as freeware in 1991, PGP has become the worldwide defacto standard for email encryption. PGP is based on public key cryptography, and allows people to exchange files or messages with privacy, authentication, and convenience.

Cryptography software involves trust—trust in the algorithms, trust in the protocols, trust in the way that keys are managed, trust in the integrity of the implementor. Somehow, PGP has become widely trusted by PGP users. Part of the reason is that Phil, right from the beginning, published the source code to PGP so that people can inspect it for "back doors", themselves. The books you hold in your hand extend that tradition of source code publication for peer review. We hope they will extend and expand the trust of PGP by the user and developer communities.

These books provide a complete copy of the source code needed to build the current release of PGP 6.5.1. In addition, they include most of the extra packaging material and installation scripts used to build the commercially distributed packages, since that portion is not completely above suspicion, either.

To ensure that the books can be clearly read, they are printed in a format recommended by the book *Tools for Publishing Source Code via OCR* (ISBN 1-891064-02-9). In addition, each of the three sets of volumes has its own file consisting of SHA hashes for each reconstructed source code file. The files of assembled hashes have been digitally signed by the Network Associates PGP Software Release Key, ultimately ensuring the authenticity of the contents of each set.

Preface

You hold in your hand one of many volumes that comprise the complete printed source code to PGP Version 6.5.1, a set numbering tens of thousands of pages. In keeping with my own long-standing tradition from the days before I started PGP, Inc., our source code is being openly published to facilitate peer review. This allows everyone to assure themselves that there are no hidden back doors that might compromise security.

Peer review of the source code for programs this large cannot be completely effective unless the expert reviewers can compile and test the software, and verify that the book-published source code behaves like the binary object code that is published electronically. To facilitate that, we publish the source code in a printed form that can be scanned in via OCR (optical character recognition) technology. This book is typeset according to the formats published in the book "Tools for Publishing Source Code via OCR" (ISBN 1-891064-02-9), by Colin Plumb, Mark Weaver, and Philip Zimmermann, 1997, available from Printers, Inc. Bookstore in Palo Alto, California.

It's nice to be able to publish these books without having to fight an extensive legal battle. As you may know, while a printed book or other printed material setting forth encryption source code is not itself subject to U.S.Export Administration Regulations, (see EAR §734.3(b)(2)), the U.S. Government says it is considering whether and to what extent scannable encryption source or object code in printed form should be subject to the regulations. We think this is rather remarkable in light of the ruling by U.S. District Court Judge Marilyn Hall Patel who said, "Source code is speech afforded the full protection of the First Amendment." Bernstein v. United States Dept. of State, 922 F. Supp. 1426, 1428-30 (N.D.Cal. 1996). In any event, according to both the export regulations and the court, the publication of these books is perfectly legal. We make these books available in bookstores for the general public to purchase. Books published this way may be exported, but only while they are still in printed form.

For those of you unfamiliar with the legal history of PGP, it's worth noting how we got here. Between 1993 and 1996 I was the target of a criminal investigation by U.S. Customs. The U.S. Government took the position that encryption software should not be exported without a license from the State Department. Since PGP was published for free on the Internet in 1991 and subsequently spread all around the world, the government assumed that the law must have been broken. That triggered the creation of a mostly pro-bono legal defense team, a legal defense fund, and three years of almost daily press interviews. The press was unanimously (!) against prosecuting and the cryptographic policy issue drew the wrath of the whole computer industry.

The first fully-implemented cryptographic software package published in its entirety in book form was "PGP Source Code and Internals" (ISBN 0-262-24039-4), by Philip Zimmermann, published by The MIT Press in 1995, during the investigation of PGP. The MIT Press informed the State Department in advance, in writing, that they were going to publish the book, and that they were going to export the book to their overseas distributors. The government raised no objections, and the book was exported without incident. My legal defense team had planned to bring this fact up at trial if I were indicted for the 1991 publication of PGP.

The investigation was closed without indictments in January 1996. Shortly after that, I started my own company, PGP, Incorporated. We hired a team of full-time engineers to develop products like PGP 5.0 and 5.5. In December 1997, PGP Inc. was acquired by Network Associates Inc. (NAI), and since then we have developed new and better versions of PGP.

Many PGP users have written and asked me if NAI has compromised the cryptographic integrity of PGP, perhaps at the government's behest. Let me assure you that since the acquisition of PGP Inc., up to the time of this writing, NAI has not shown even the remotest interest in compromising the security of PGP, and I don't expect that to change. In fact, NAI has a strong financial interest in keeping strong crypto in PGP

products because that's what PGP customers want. Further, I'd like to point out that when NAI acquired PGP, they didn't just acquire a product. They also acquired a team of people who were already dedicated to the principles of personal privacy. And let me assure the reader that for as long as I am associated with NAI, I will personally continue to work with the rest of the PGP team to ensure the cryptographic integrity of PGP.

Philip Zimmermann
prz@pgp.com
31 July 1999

General Build Instructions

For the Macintosh or Windows platforms, please see the platform-specific build instructions.

The LDAP source code here is from the University of Michigan. For publication, we have not included the MS-DOS and VMS specific portions of the code, although there is no reason that you could not add them back in.

There are two 'extras' included in this book. One is the *shasum* perl script used to generate the SHA hashes in this series. It is like the *md5sum* program, but generates SHA hashes. To use it, you will need the SHA package for Perl, readily available from the net, e.g. http://www.perl.org/. Note that the hashes are computed using the 'new' SHA-1 hash, which is *not* the default supplied by the SHA-1.1 package.

The second extra is a trivial patch to the *sortpages* utility from *Tools for Publishing Source Code via OCR*, without which it will reject binary files.

The source code in this book is the common source code needed by the Macintosh and Windows builds. All of the code needed to build the command-line versions of PGP 6.5.1 are also contained within these volumes, with the exception of the command-line versio of PGP for Windows, which also requires the Windows platform source code book.

Windows Build Instructions

Build requirements

The following third-party tools/SDKs are needed to build PGP 6.5.1:

- Microsoft Visual C++ 6.0 (http://www.microsoft.com)
- Microsoft Visual Studio 6.0 Service Pack 2
- InstallShield 5.5 Professional (http://www.installshield.com)
- InstallShield 5.5 Maintenance Pack 3 (http://www.installshield.com)

Preparing the build environment

(1) Install Microsoft Visual C++ 6.0. Perform a "Custom" install and install all components except the online books.

(2) Install the remaining build tools:

- Microsoft Visual Studio 6.0 Service Pack 2
- InstallShield
- InstallShield Maintenance Pack 3

Preparing the source code tree

All of the binaries are located in the zip files of the name "binaresXXX.zip". The common source code has two such files ("binariesA.zip" and "binariesB.zip") and the Windows source code has two ("binaries1.zip" and "binaries2.zip"). These files contain the binaries in a "parallel" hierarchy to the source tree. Use your favorite zip utility to decompress these archives into the "clients" and "libs" directories.

Setting source code flags

The following library flags are located in "libs/pgpcdk/priv/include/pgpSDKBuildFlags.h":

- PGP_RSA: Set to 1 for RSA-enabled builds
- PGP_RSA_KEYGEN: Set to 1 to allow RSA key generation
- PGP_USECAPIFORRSA: Set to 1 to use Microsoft's Crypto API (CAPI) for RSA operations.
- PGP_USECAPIFORMD2: Set to 1 to use Microsoft's Crypto API (CAPI) for MD2 hashing operations.
- PGP_USEBSAFEFORRSA: Set to 1 to use RSA's BSAFE library for RSA operations. Note that BSAFE is not included in these source code books.
- PGP_USEPGPFORRSA: Set to 1 to use the PGP implementation for RSA operations.
- PGP_USERSAREF: Set to 1 to use the RSAREF library for RSA operations. Note that RSAREF is not included in these source code books.

These flags should be set as follows for all three of the supported builds: PGP_RSA = 1, PGP_RSA_KEYGEN = 1, PGP_USECAPIFORRSA = 0, PGP_USECAPIFORMD2 = 0, PGP_USEBSAFEFORRSA = 0, PGP_USEPGPFORRSA = 1, PGP_USERSAREF = 0.

Building the code

(1) Open the workspace file "clients/pgp/cmdline/PGPcmd.dsw" and make the "Win32 Release" configuration of the "PGPcmd" project.

(2) Close "PGPcmd.dsw", open the workspace file "clients/pgp/win32/MakeSEA.dsw", and make the "Win32 Release" configuration of the "MakeSEA" project.

Building the installer

(1) Open a command prompt window and navigate to the directory "clients/pgp/cmdline/packaging/Install/".

(2) Execute the batch file "CopyFiles.bat". This batch file copies all relevant files from the build directories into the install directories. This batch file takes an optional parameter "FREEWARE" if a freeware build is desired.

(3) Open the InstallShield Pro project file "clients/pgp/cmdline/packaging/Install/PGP 6.5 CmdLN NT.ipr" and choose "Media->Media Build Wizard..." from the **Build** menu.

(4) Click the **Next** button.

(5) Choose "CD-ROM" from the media types list and click the **Next** button.

(6) Choose the "Full Build" option and click the **Next** button.

(7) Continue to click the **Next** button and accept the defaults for subsequent wizard panels.

(8) Click the **Finish** button after the installer has been built and close the InstallShield project file "PGP 6.5 CmdLN NT.ipr".

(9) Copy the directory "clients/pgp/cmdline/packaging/Install/Media/New Media/Disk Images/" to a temporary directory.

(10) Copy the file "clients/pgp/win32/MakeSEA/Release/MakeSEA.exe"' to the temporary directory created in the previous step.

(11) Open a command prompt window and navigate to the tempory directory created above.

(12) Execute the following command. Note the need for quotation marks around the last parameter: makesea.exe Setup.exe ".\Disk Images". This will create the packaged installer "Setup.exe".

End of Windows build instructions.

Solaris 2.5.1 Build Instructions

Build requirements

The following third-party tools/SDKs are needed to build PGP 6.5.1 for Solaris 2.5.1:

- gcc/g++ version 2.8.1
- autoconf version 2.12
- GNU make version 3.75

Preparing the source code tree

All of the binaries are located in the zip files "binariesA.zip" and "binariesB.zip". These files contain the binaries in a "parallel" hierarchy to the source tree. Unzip these archives into the "clients", "libs", and "docs" directories.

Setting source code flags

The following library flags are located in "libs/pgpcdk/priv/include/pgpSDKBuildFlags.h":

- PGP_RSA: Set to 1 for RSA-enabled builds
- PGP_RSA_KEYGEN: Set to 1 to allow RSA key generation
- PGP_USECAPIFORRSA: Set to 1 to use Microsoft's Crypto API (CAPI) for RSA operations.
- PGP_USECAPIFORMD2: Set to 1 to use Microsoft's Crypto API (CAPI) for MD2 hashing operations.
- PGP_USEBSAFEFORRSA: Set to 1 to use RSA's BSAFE library for RSA operations. Note that BSAFE is not included in these source code books.
- PGP_USEPGPFORRSA: Set to 1 to use the PGP implementation for RSA operations.
- PGP_USERSAREF: Set to 1 to use the RSAREF library for RSA operations. Note that RSAREF is not included in these source code books.

These flags should be set as follows for PGP 6.5.1: PGP_RSA = 1, PGP_RSA_KEYGEN = 1, PGP_USECAPIFORRSA = 0, PGP_USECAPIFORMD2 = 0, PGP_USEBSAFEFORRSA = 0, PGP_USEPGPFORRSA = 1, PGP_USERSAREF = 0.

Building the code

(1) Set the command prompt to the directory "clients/pgp/cmdline/".

(2) Change the mode flags of the file "clients/pgp/cmdline/build.sh" to allow execution with "chmod +x ./build.sh".

(3) Execute the build script with "./build.sh SOLARIS". If a freeware version is being built, use the command "./build.sh SOLARIS FREE".

The build result will be the a Solaris installation package file "clients/pgp/cmdline/packaging/pgp-6.5.1-sol".

End of Solaris build instructions.

Build requirements

The following third-party tools/SDKs are needed to build PGP 6.5.1 for Red Hat Linux 5.2:

- gcc version 2.7.2.3
- g++ version egcs-1.0.3
- autoconf version 2.12
- GNU make version 3.76

Note: The PGP command line product will not compile with Red Hat Linux 6.0.

Preparing the source code tree

All of the binaries are located in the zip files "binariesA.zip" and "binariesB.zip". These files contain the binaries in a "parallel" hierarchy to the source tree. Unzip these archives into the "clients", "libs", and "docs" directories.

Setting source code flags

The following library flags are located in "libs/pgpcdk/priv/include/pgpSDKBuildFlags.h":

- PGP_RSA: Set to 1 for RSA-enabled builds
- PGP_RSA_KEYGEN: Set to 1 to allow RSA key generation
- PGP_USECAPIFORRSA: Set to 1 to use Microsoft's Crypto API (CAPI) for RSA operations.
- PGP_USECAPIFORMD2: Set to 1 to use Microsoft's Crypto API (CAPI) for MD2 hashing operations.
- PGP_USEBSAFEFORRSA: Set to 1 to use RSA's BSAFE library for RSA operations. Note that BSAFE is not included in these source code books.
- PGP_USEPGPFORRSA: Set to 1 to use the PGP implementation for RSA operations.
- PGP_USERSAREF: Set to 1 to use the RSAREF library for RSA operations. Note that RSAREF is not included in these source code books.

These flags should be set as follows for PGP 6.5.1: PGP_RSA = 1, PGP_RSA_KEYGEN = 1, PGP_USECAPIFORRSA = 0, PGP_USECAPIFORMD2 = 0, PGP_USEBSAFEFORRSA = 0, PGP_USEPGPFORRSA = 1, PGP_USERSAREF = 0.

Building the code

(1) Set the command prompt to the directory "clients/pgp/cmdline/".

(2) Change the mode flags of the file "clients/pgp/cmdline/build.sh" to allow execution with "chmod +x ./build.sh".

(3) Execute the build script with "./build.sh LINUX". If a freeware version is being built, use the command "./build.sh LINUX FREE".

The build result will be the tar file "clients/pgp/cmdline/packaging/pgp-6.5.1-linux-rsa.i386".

End of Linux build instructions.

AIX 4.2 Build Instructions

Build requirements

The following third-party tools/SDKs are needed to build PGP 6.5.1 for AIX 4.2:

- gcc/g++ version 2.8.1
- autoconf version 2.12
- GNU make version 3.75

Preparing the source code tree

All of the binaries are located in the zip files "binariesA.zip" and "binariesB.zip". These files contain the binaries in a "parallel" hierarchy to the source tree. Unzip these archives into the "clients", "libs", and "docs" directories. The AIX build requires the application of a source code patch to the reconstructed source files. This patch is located in the file "aix-hpux.patch". This will update several source files in the "clients" and "libs" directories. This patch was created on the Solaris operating system and may require a Solaris-compatible version of the patch utility to work correctly.

Setting source code flags

The following library flags are located in "libs/pgpcdk/priv/include/pgpSDKBuildFlags.h":

- PGP_RSA: Set to 1 for RSA-enabled builds
- PGP_RSA_KEYGEN: Set to 1 to allow RSA key generation
- PGP_USECAPIFORRSA: Set to 1 to use Microsoft's Crypto API (CAPI) for RSA operations.
- PGP_USECAPIFORMD2: Set to 1 to use Microsoft's Crypto API (CAPI) for MD2 hashing operations.
- PGP_USEBSAFEFORRSA: Set to 1 to use RSA's BSAFE library for RSA operations. Note that BSAFE is not included in these source code books.
- PGP_USEPGPFORRSA: Set to 1 to use the PGP implementation for RSA operations.
- PGP_USERSAREF: Set to 1 to use the RSAREF library for RSA operations. Note that RSAREF is not included in these source code books.

These flags should be set as follows for PGP 6.5.1: PGP_RSA = 1, PGP_RSA_KEYGEN = 1, PGP_USECAPIFORRSA = 0, PGP_USECAPIFORMD2 = 0, PGP_USEBSAFEFORRSA = 0, PGP_USEPGPFORRSA = 1, PGP_USERSAREF = 0.

Building the code

(1) Set the command prompt to the directory "clients/pgp/cmdline/".

(2) Change the mode flags of the file "clients/pgp/cmdline/build.sh" to allow execution with "chmod +x ./build.sh".

(3) Execute the build script with "./build.sh AIX". If a freeware version is being built, use the command "./build.sh AIX FREE".

The build result will be the tar file "clients/pgp/cmdline/packaging/pgp-6.5.1-aix-rsa.tar".

End of AIX build instructions.

Build requirements

The following third-party tools/SDKs are needed to build PGP 6.5.1 for HP-UX 10.20:

- gcc/g++ version 2.8.1
- autoconf version 2.13
- GNU make version 3.77

Preparing the source code tree

All of the binaries are located in the zip files "binariesA.zip" and "binariesB.zip". These files contain the binaries in a "parallel" hierarchy to the source tree. Unzip these archives into the "clients", "libs", and "docs" directories. The HP-UX build requires the application of a source code patch to the reconstructed source files. This patch is located in the file "aix-hpux.patch". This will update several source files in the "clients" and "libs" directories. This patch was created on the Solaris operating system and may require a Solaris-compatible version of the patch utility to work correctly.

Setting source code flags

The following library flags are located in "libs/pgpcdk/priv/include/pgpSDKBuildFlags.h":

- PGP_RSA: Set to 1 for RSA-enabled builds
- PGP_RSA_KEYGEN: Set to 1 to allow RSA key generation
- PGP_USECAPIFORRSA: Set to 1 to use Microsoft's Crypto API (CAPI) for RSA operations.
- PGP_USECAPIFORMD2: Set to 1 to use Microsoft's Crypto API (CAPI) for MD2 hashing operations.
- PGP_USEBSAFEFORRSA: Set to 1 to use RSA's BSAFE library for RSA operations. Note that BSAFE is not included in these source code books.
- PGP_USEPGPFORRSA: Set to 1 to use the PGP implementation for RSA operations.
- PGP_USERSAREF: Set to 1 to use the RSAREF library for RSA operations. Note that RSAREF is not included in these source code books.

These flags should be set as follows for PGP 6.5.1: PGP_RSA = 1, PGP_RSA_KEYGEN = 1, PGP_USECAPIFORRSA = 0, PGP_USECAPIFORMD2 = 0, PGP_USEBSAFEFORRSA = 0, PGP_USEPGPFORRSA = 1, PGP_USERSAREF = 0.

Building the code

(1) Set the command prompt to the directory "clients/pgp/cmdline/".

(2) Change the mode flags of the file "clients/pgp/cmdline/build.sh" to allow execution with "chmod +x ./build.sh".

(3) Execute the build script with "./build.sh HPUX". If a freeware version is being built, use the command "./build.sh HPUX FREE".

The build result will be the tar file "clients/pgp/cmdline/packaging/pgp-6.5.1-hpux-rsa.tar".

End of HP-UX build instructions.