
RSA BSAFE[®] CRYPTO-C 4.2

Release Notes

An RSA Engineering Note
June 2, 1999

This note summarizes the features of the RSA BSAFE[®] Crypto-C 4.2 software, the contents of the distribution package, and the changes from prior releases of Crypto-C.

New Features in RSA BSAFE Crypto-C 4.2

RSA BSAFE Crypto-C 4.2 is an update to BSAFE Crypto-C 4.1 that provides improved security via the following features:

- (Windows 95, 98, and NT only) Support for the Intel[®] hardware security features, which currently include the Intel Random Number Generator (RNG). For information on the Intel security features, including how to access the RNG from Crypto-C, and how to redistribute the Intel driver, see the *RSA BSAFE Crypto-C Intel Security Hardware User's Guide*.
- Support for random number generation with six independent streams of randomness, as described in the X9.31 standard.
- Support for DSA public and private keys in the ANSI X9.57 BER format.
- Crypto-C source files for Unix platforms (HP-UX and Solaris) are now compiled to produce position-independent code libraries. This change will enable developers of shared objects to use the Crypto-C SDK without having to obtain a special library from RSA Data Security, Inc. Other users of Crypto-C will not be affected. If your application uses shared objects, please ensure you abide by the restrictions stated in the commercial license from RSA Data Security, Inc.
- (HP-UX only) Support for qualified 64-bit versions of the PA-RISC 2.0 platforms. Note that 32-bit versions of the Crypto-C library are available for both the PA-RISC 1.1 and PA-RISC 2.0 platforms, while an ELF 64 Object File Format version of the Crypto-C library runs on qualified 64-bit PA-RISC 2.0 platforms. On the PA-RISC 2.0 platforms, both the 32-bit and the 64-bit version contain assembly multiplication routines that greatly accelerate RSA operations.

Getting Started

The directions for getting started with RSA BSAFE Crypto-C 4.2 are the same as with previous releases. The media contains the header and Crypto-C library files that can be compiled and linked with your products. It also contains a directory with several demo programs and a `readme` file with the latest information, as well as a FIPS folder with the FIPS-compliant module and test vectors.

Backward compatibility is a major feature of BSAFE 4.2, so you can try it out by recompiling your application with the new header files and relinking with the new library file.

The media contains:

- Compiler-specific declarations in `aglobal.h`
- Crypto-C type declarations in `atypes.h`
- Crypto-C application interface in `bsafe.h`
- Object library: `bsafe42.lib` (on Windows) or `libbsafe.a` (on UNIX)
- Demo programs in the `library\make sub-directory`
- (Windows 95, 98, NT only) The redistribution package for the Intel hardware security features in the `bsafe42\Redistrib` directory.
- `.pdf` files for the entire range of current PKCS documents, appearing in the `bsafe42\doc\other\` directory.
- `.pdf` files reflecting the latest version of the manuals, as well as a new manual, the *RSA BSAFE Crypto-C 4.2 Intel Security Hardware User's Guide*, all appearing in the `bsafe42\doc\` directory.

Installation Instructions

Note: If you do not have a CD-ROM Drive attached to your computer, please consult the system administrator for your local machine.

Windows 95, Windows 98, and Windows NT Users:

This procedure assumes that your CD-ROM drive is Drive D:. If it is a different drive, change the examples accordingly.

- Insert the Crypto-C CD into the CD-ROM drive.
- In Windows Explorer, change to drive D:.
- Change to the folder `Win32`, and choose `Setup`.
- InstallShield will take you through the installation process for your system.

Solaris Users:

This procedure assumes that the *vold* daemon is running. If it is not, contact your local system administrator to start it or to install the toolkit. By default, *vold* uses a mountpoint of `/cdrom/<cdromlabel>`. This example assumes that the label for the CD-ROM is `42rell`.

- Insert the Crypto-C CD into the CD-ROM drive. *vold* should automatically mount the CD-ROM on the file system. The default location is underneath the directory `/cdrom`.
- Open a terminal window and type the command: `mount`. This command lists all file systems currently mounted by the operating system. There should be one that starts with `/cdrom`. This is the mountpoint for the CD-ROM.
- The program files for AIX, Solaris and HP-UX are contained in the file `bsafe42.tar`. This is a tar archive that contains a number of demo and sample programs, along with the Crypto-C 4.2 library. To view these files, `untar` the `bsafe42.tar` archive with the Unix™ `tar` command. For example, if the CD was mounted on the directory `/cdrom/bsafe42`, you would use the command:

```
tar xvf /cdrom/bsafe42/bsafe42.tar
```

to extract files from the archive.

AIX and HP-UX Users:

- Insert the Crypto-C CD into the CD-ROM drive.
- Open a terminal window and type the command: `mount`. For example, if you want to mount the CD at the mountpoint `/cdrom/bsafe42`, use the command:

```
mount /dev/hdc /cdrom/bsafe42
```

- The program files for UNIX are contained in the file `bsafe42.tar`. This is a tar archive that contains a number of demo and sample programs, along with the Crypto-C 4.2 library. To view these files, untar the `bsafe42.tar` archive with the Unix™ `tar` command. For example, if the CD was mounted on the directory `/cdrom/bsafe42`, you would use the command:

```
tar xvf /cdrom/bsafe42/bsafe42.tar
```

to extract files from the archive.

The Command-Line Demos

The demo programs located in the `library\make` subdirectory are command-line applications that demonstrate some of the aspects of building cryptographic applications using Crypto-C. They use the Crypto-C 4.2 library routines and are provided to Crypto-C customers in source form.

Note to UNIX users only

The `library\make` directory is non-writeable on UNIX systems. When running a demo, UNIX users should make sure that intermediate files are saved to a writeable directory. This means that whenever you are prompted for the name of a file where data will be saved, you should make sure you specify a path to a file in another, writeable, directory.

For example, when signing a file with **bdemo**, at the prompt to save the signature (the second prompt which appears):

```
> Enter filename to save the signature <blank to cancel>:
```

you might enter:

```
/tmp/signature
```

Changes in Crypto-C 4.2

- A new hardware method provides support for the Intel Random Number Generator: HW_INTEL_RANDOM.
- New key info types support X9.57 BER-encoding for the DSA algorithm. They include: KI_DSAPrivateX957BER and KI_DSAPublicX957BER.
- A new algorithm info type, AI_X931Random which supports X9.31 random number generation with six streams of randomness. This is intended primarily for use with the existing AI, AI_RSAStrongKeyGen.

Key Sizes In Crypto-C 4.2

This release of Crypto-C supports the following keyed cryptographic algorithms:

Algorithm	Effective Key Bits
DES	56
DESX	120
Triple-DES	168
RC2	1-1024
RC4	8-2048
RC5	8-2048
RSA	256-2048
Diffie-Hellman	128-2048
DSA	512-2048

For a full listing of other algorithms and details on usage, please consult the *Crypto-C Library Reference Manual*.

Notes for Source Code Users

The Crypto-C distribution contains a `bsfplatf.h` specific to your platform. This file is located in the `make` directory for your platform in the `toolkit\make` directory tree. To build Crypto-C for your platform, you must copy `bsfplatf.h` to the `toolkit\bsource\include` directory and use the `Makefile` for your platform.

Visual C++ 6.0 and Crypto-C

In some circumstances, the Visual C++ 6.0 compiler generates bad code when optimizations are enabled. Bugs can appear when Crypto-C sources are compiled with VC 6.

Microsoft has released a new service pack for Visual Studio 6.0 (of which Visual C++ is a component) that fixes this optimization bug. The URL for Visual C++ is <http://msdn.microsoft.com/visualc>. Follow the link from this web page to the Service Pack 3 download area.

About Support

RSA Data Security, Inc. is committed to helping you effectively integrate our security into your applications. For details on our support plans, please contact a Telesales Representative at 650-295-7600, or view our support options online at <http://support.rsa.com>.