

The cryptography "gold standard" of professional developers worldwide

# BSAFE™ 3.0 RSA's comprehensive cryptography engine for software developers

## Introducing BSAFE 3.0

BSAFE 3.0 is the newest release of the world's most popular cryptography toolkit. Fully compatible with keys and data from previous versions, BSAFE 3.0 is a portable C programmer's toolkit that allows developers to integrate state-of-the-art privacy and authentication features into virtually any application. BSAFE 3.0 provides the programmer with a complete palette of the most popular and trusted cryptographic algorithms, including Triple-DES, RC5, and of course the patented RSA Public Key Cryptosystem™, the worldwide standard for Internet security. New in BSAFE 3.0 is support for the DSA and SHA1 U.S. government signature and hashing algorithms.

## Easy, Full-Featured Development Environment

BSAFE 3.0 can dramatically reduce the cost associated with development of secure applications by giving developers a big head start. With BSAFE, any programmer can develop secure applications — without a background in cryptography, mathematics or number theory. Best of all, by using the toolkit from the most trusted and experienced company in the cryptography business, you won't be troubled by embarrassing and costly software recalls that often result from failed "homegrown" security techniques. BSAFE features an object-oriented API utilizing data abstraction, providing for more efficient development. BSAFE 3.0 is also re-entrant, so it can be shared by many applications at once — a necessity in today's advanced multi-

tasking operating environments. Long, computationally-intensive cryptographic operations are interruptible or even cancelable, and there are a variety of platform-specific optimizations available.

## Algorithms: Flexibility and Performance

BSAFE 3.0 includes routines for the patented RSA and Diffie-Hellman public-key techniques; the DSA government signature algorithm; the popular DES, Triple-DES and DESX secret-key ciphers; the exportable RC2 and RC4 variable key size ciphers; the high-performance RC5 symmetric block cipher; Bloom-Shamir secret sharing and key escrow; the MD2, MD5 and SHA1 hashing algorithms; and improved routines for pseudorandom number generation. And you'll be able to use these algorithms at unprecedented levels of performance — algorithms that function up to 5 times faster than previous versions of BSAFE. That means with BSAFE you'll be able to implement high-bandwidth crypto applications, like secure video, totally in software — without resorting to expensive special-purpose crypto hardware.

## What about Standards?

BSAFE is the world's best-selling crypto toolkit, so naturally it can support virtually any global security standard — in fact, many standards were written around the BSAFE toolkit! That means you can talk securely to just about anybody, whether they're speaking SSL, S/HTTP, SEPP, STT, S/MIME, S/WAN, IPsec or PCT. And of course, BSAFE fully supports PKCS, (the Public Key Cryptography Standards) the internationally-recognized public-key interoperability specifications.

## Ready for the Future

BSAFE 3.0 was designed to be modular, so you can link in only the algorithms you need. It's also extensible, so you can insert new algorithms in the future — no matter where technology or government specifications take you. BSAFE also supports multiple key and data representations including previous BSAFE 1.x formats, BSAFE 2.x formats and ASN.1 BER (Basic Encoding Rules). Consequently, development is faster and applications built with BSAFE 3.0 enjoy better "forward compatibility" with future encryption techniques and standards.

## Unbeatable References

Some of the world's most talented development teams chose RSA's BSAFE toolkit to provide the cryptography built into all of these best-selling applications:

### Novell Network™

*secure network operating system*

### Netscape Navigator™ Browsers & Electronic Commerce Servers

*secure Internet browsers and servers*

### Lotus Notes™

*secure workgroup software*

### Digital Internet Tunnel™

*secure VPN via the Internet*

### Oracle SQL\*Net™

*secure client/server database*

### Microsoft Windows 95™

*operating system security*

...and many, many more. Your application can be on this list, too. With BSAFE, your developers can bring the security benefits of professional cryptography into any application you wish to build — quickly, easily and inexpensively.



# BSAFE 3.0 Specifications

## Features

- General purpose, low-level cryptography engine
- Backwards-compatible with BSAFE 1.x and BSAFE 2.x keys and data
- Supports the Public Key Cryptography Standards (PKCS)
- Suitable for real-time encryption/authentication applications
- Supports the following cryptographic techniques:
  - RSA Public Key Cryptosystem
  - RSA Digital Signatures
  - Diffie-Hellman Key Agreement
  - Digital Signature Algorithm (DSA/DSS)
  - Data Encryption Standard (DES)
  - Triple-DES
  - Extended Data Encryption Standard (DESX)
  - RC2 Variable-Key Size Symmetric Block Cipher
  - RC4 Variable-Key Size Symmetric Stream Cipher
  - RC5 Variable-Key Size Symmetric Stream Cipher
  - MD Hashing Algorithm
  - MD2 Hashing Algorithm
  - MD5 Hashing Algorithm
  - SHA1 Hashing Algorithm
- Supports user-definable key sizes up to 2048 bits
- Modular and extensible algorithm framework can easily accommodate new algorithms and standards as needed
- Object-oriented, portable C API
- Re-entrant, interruptible and cancelable cryptographic operations
- Hardware-specific algorithm optimizations available
- Support for multiple key and data representations including ASN.1 BER

## Potential BSAFE 3.0 Applications

- Secure Internet Browsers and Servers
- Encrypted Electronic Mail
- Secure Electronic Commerce
- Client/Server Security
- Encryption of Local & Archived Files
- Network User and Service Authentication
- Kerberos Enhancement and Extension
- Secure Software Distribution (CD-ROM)
- Broadcast Encryption
- Voice and Video Encryption
- Digitally Signed Electronic Forms & Workflow
- Encrypted Database and other Client/Server Applications
- Intellectual Property Protection
- Virus Detection
- Secure Remote Access and TCP/IP

## System Requirements

Platforms: DOS, Windows, Windows 95, Windows NT, OS/2, Macintosh, AT&T SVR4 UNIX (Intel), HP/UX, SunOS, Solaris, IBM AIX, NeXT, Silicon Graphics, SCO UNIX, Alpha VMS, VAX VMS, ports to other platforms available.

Memory: 5-20K per algorithm used, application dependent

## Related RSA Product Offerings

End-users requiring an application that provides integrated encryption and emergency access capabilities for file and document security should examine RSA Secure, RSA's award-winning file system security extension.

Developers needing to integrate security into store-and-forward based messaging applications like e-mail, e-forms, EDI or electronic commerce should consider TIPEM, RSA's standards-based Toolkit for Interoperable Privacy-Enhanced Messaging.

## Developer & Runtime Pricing

See the latest RSA Price Sheet for individual, 5-user and 10-user developer object-code pricing, and quantity runtime distribution pricing.

## RSA Licensing

BSAFE 3.0 object or source code can be inexpensively licensed from RSA for inclusion in an application that you intend to market. Royalties and license terms depend on your application type. Contact your RSA representative for a copy of our standard license agreement and a quote.

## Contacting RSA



RSA Data Security, Inc.  
100 Marine Pkwy Ste. 500  
Redwood City, CA 94065  
Phone: 415-595-8782  
Facsimile: 415-595-1873  
info@rsa.com  
<http://www.rsa.com/>

RSA products contain proprietary, confidential, and/or trade secret RSA encryption algorithms and subroutines. Applications developed with RSA products, if distributed or sold, are subject to additional licensing. Source code licensing is also available. Contact RSA for details.

Copyright © 1996 RSA Data Security, Inc.  
All rights reserved. The RSA Public Key Cryptosystem is protected under U.S. Patent # 4,405,829.