RSA BSAFE®

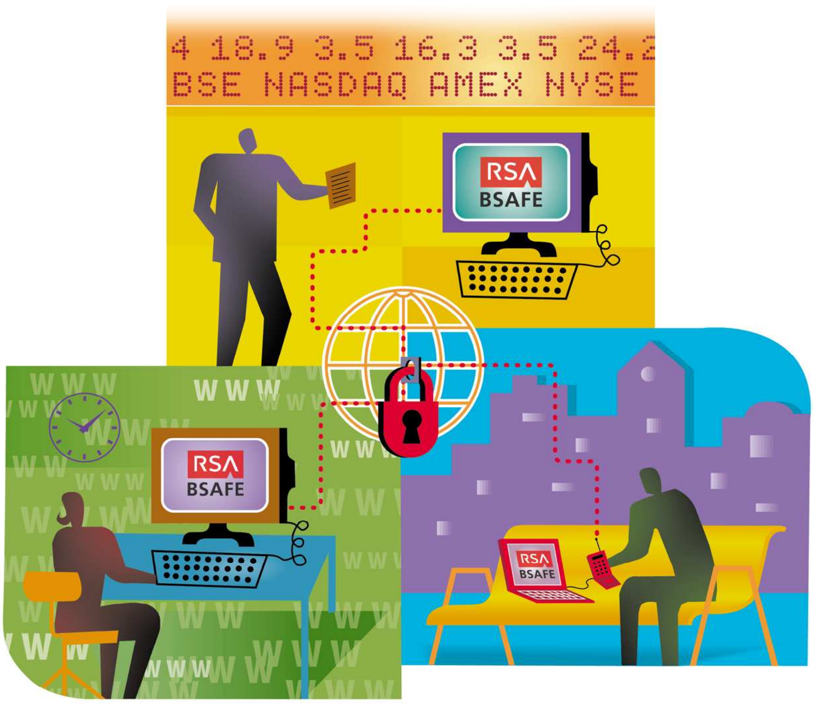
Crypto-C ME

Security Policy

Version 1.9.0

September 7, 2005

Powerful cryptography for the smallest of devices



RSA SECURITY®

Contact Information

See our Web sites for regional Customer Support telephone and fax numbers.

RSA Security Inc.	RSA Security Ireland Limited
www.rsasecurity.com	www.rsasecurity.ie

Trademarks

ACE/Agent, ACE/Server, Because Knowledge is Security, BSAFE, ClearTrust, Confidence Inspired, e-Titlement, IntelliAccess, Keon, RC2, RC4, RC5, RSA, the RSA logo, RSA Secured, the RSA Secured logo, RSA Security, SecurCare, SecurID, SecurWorld, Smart Rules, The Most Trusted Name in e-Security, Transaction Authority , and Virtual Business Units are either registered trademarks or trademarks of RSA Security Inc. in the United States and/or other countries. All other goods and/or services mentioned are trademarks of their respective companies.

License Agreement

This software and the associated documentation are proprietary and confidential to RSA Security, are furnished under license and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright below. This software and any copies thereof may not be provided or otherwise made available to any other person.

Neither this software nor any copies thereof may be provided to or otherwise made available to any third party. No title to or ownership of the software or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by RSA Security.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import or export of encryption technologies and current use, import and export regulations should be followed when exporting this product.

Distribution

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

RSA Security Notice

The RC5® Block Encryption Algorithm With Data-Dependent Rotations is protected by U.S. Patent #5,724,428 and #5,835,600.

Compaq MultiPrime™ technology is protected by U.S. Patent #5,848,159 and is the subject of patent applications in other countries.

This product includes patented technology licensed from Entrust Technologies Inc. (US Patent# 5,699,431).

Published September 7, 2005

001-001004-190-002-000

Table of Contents

1. Introduction

This is a non-proprietary RSA Security Cryptographic Module security policy. This security policy describes how the Cryptographic Module meets the security requirements of FIPS 140-2, and how to securely operate the Cryptographic Module in a FIPS-compliant manner. This policy was prepared as part of the level 1 FIPS 140-2 validation of the Cryptographic Module.

FIPS 140-2 (Federal Information Processing Standards Publication 140-2 — *Security Requirements for Cryptographic Modules*) details the United States Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the NIST Web site at http://csrc.nist.gov/cryptval/.

2. References

This document deals only with operations and capabilities of the Crypto-C ME module in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the Crypto-C ME module and the entire RSA BSAFE product line from the following resources:

- The RSA website contains information on their full line of products and services at http://www.rsasecurity.com/.
- An overview of the Crypto-C ME module is located at http://www.rsasecurity.com/node.asp?id=1210.
- The RSA BSAFE product overview is provided at http://www.rsasecurity.com/node.asp?id=1202.
- For answers to technical or sales related questions please refer to http://www.rsasecurity.com/contact/.

3. Document Organization

This document explains the Cryptographic Module's FIPS 140-2 relevant features and functionality. This first section, Introduction, provides an overview and introduction to the Security Policy. Crypto-C ME Module on 5 describes the Cryptographic Module and how it meets FIPS 140-2 requirements.

Secure Operation of the Cryptographic Module on page 11 specifically addresses the required configuration for the FIPS-mode of operation. Services on page 13 lists all of the functions provided by the Cryptographic Module. Acronyms on page 16 lists the definitions for the acronyms used in this document.

4. Crypto-C ME Module

This section provides an overview of the Crypto-C ME Module. The following topics are discussed:

- Introduction
- Cryptographic Module
- Module Interfaces
- Roles and Services
- Cryptographic Key Management
- Cryptographic Algorithms
- Self-Test.

4.1. Introduction

Wireless technology provides easy and fast delivery of information and services through handheld digital devices such as mobile phones, pagers and personal digital assistants (PDAs). Crypto-C Micro Edition can be easily ported to different embedded operating systems and its features include the ability to optimize code for different processors and for specific speed or size requirements (Note: When operating in a FIPS-approved manner, the set of algorithm implementations is not customizable).

Crypto-C Micro Edition offers a full set of cryptographic algorithms, including public key operations, symmetric, block and stream ciphers, message digests, message authentication and the Pseudo Random Number Generator (PRNG). Developers can implement the full suite of algorithms through a single Application Programming Interface (API) or select a specific set of algorithms in order to meet performance or resource constraints.

With Crypto-C Micro Edition, companies can easily embed high levels of security and privacy into a wide range of wireless applications without being cryptography experts.

4.2. Cryptographic Module

This Cryptographic Module is classified as a multi-chip standalone module for FIPS 140-2 purposes. As such, the module must be tested upon a particular operating system and computer platform. The cryptographic boundary thus includes the Cryptographic Module running on selected platforms running selected operating systems while configured in “single user” mode. The Cryptographic Module was validated as meeting all FIPS 140-2 level 1 security requirements, including cryptographic key management and operating system requirements. The Cryptographic Module is packaged as a dynamically loaded module or shared library file which contains all the module’s executable code. Additionally, the RSA BSAFE Crypto-C ME toolkit relies on the physical security provided by the host PC in which it runs.

The RSA BSAFE Crypto-C ME toolkit was tested on the following platforms:

- Red Hat Linux 7.2 x86 (32-bit)
  Compliance is maintained on platforms for which the binary executable remains unchanged including (but not limited to):
  - Red Hat Linux 7.1, and 8.0
  - Red Hat Advanced Server 2.1.

- Red Hat Enterprise Linux AS 3.0 x86 (32-bit)
  Compliance is maintained on platforms for which the binary executable remains unchanged.

- Sun Microsystems Solaris 8 (Sun OS 5.8) Sparc V8+ (32-bit)
  Compliance is maintained on platforms for which the binary executable remains unchanged including (but not limited to):
  - Sun Microsystems Solaris 8 v8+ (32-bit).

- Sun Microsystems Solaris 8 (SunOS 5.8) Sparc V9 (64-bit)
  Compliance is maintained on platforms for which the binary executable remains unchanged including (but not limited to):
  - Sun Microsystems Solaris 9 (SunOS 5.9) Sparc V9.

- Microsoft Windows Pocket PC 2003 ARM
  Compliance is maintained on platforms for which the binary executable remains unchanged including (but not limited to):
  - SmartPhone ARM (32-bit).

- Microsoft Windows 2000 Service Pack 4
  Compliance is maintained on platforms for which the binary executable remains unchanged including (but not limited to):
  - Microsoft Windows NT 4
  - Microsoft Windows XP
  - Microsoft Windows 2003 Server.
- IBM AIX 5L v5.2 (32bit)
  Compliance is maintained on platforms for which the binary executable remains unchanged.

- HP-UX 11.0 and HP-UX 11.11 PA-RISC 2.0 (32-bit)
  Compliance is maintained on platforms for which the binary executable remains unchanged including (but not limited to):
  - HP-UX 11.0 through 11.23 for PA-RISC 2.0 processors.

- HP-UX 11.0 and HP-UX 11.11 PA-RISC 2.0W (64-bit)
  Compliance is maintained on platforms for which the binary executable remains unchanged including (but not limited to):
  - HP-UX 11.0 through 11.23 for PA-RISC 2.0 processors.

- VxWorks 5.4 PPC 604 (32-bit).
  Compliance is maintained on platforms for which the binary executable remains unchanged.

- VxWorks 5.5 PPC 603 (32-bit).
  Compliance is maintained on platforms for which the binary executable remains unchanged.
- VxWorks 5.5 PPC 604 (32-bit).
  Compliance is maintained on platforms for which the binary executable remains unchanged.

Refer to the NIST document, *Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program*, for resolution on the issue of "Multi user" modes. This document is located at: http://csrc.nist.gov/cryptval/140-1/FIPS1402IG.pdf.

4.3. Module Interfaces

The Cryptographic Module is evaluated as a multi-chip, standalone, module. The Cryptographic Module's physical interfaces consist of the keyboard, mouse, monitor, CD-ROM drive, floppy drive, serial ports, USB ports, COM ports, and network adapter(s). However, the module sends/receives data entirely through the underlying logical interface, a C-language API documented in the Cryptographic Module API Reference. The module provides for Control Input through the API calls. Data Input and Output are provided in the variables passed with API calls, and Status Output is provided through the returns, exceptions, and error codes that are documented for each call.

4.4. Roles and Services

The Crypto-C ME module meets all FIPS140-2 level 1 requirements for Roles and Services, implementing both a Crypto-User (User) role and Crypto-Officer (CO) role. As allowed by FIPS 140-2, the Crypto-C ME module does not support user identification or authentication for these roles. Only one role may be active at a time and the Crypto-C ME module does not allow concurrent operators.

Table 1 - Crypto-C ME roles and services.

Role	Services
Crypto Officer	The Crypto Officer has access to a superset of the services that are available to the Crypto User. The Officer role may also invoke the full set of self tests inside the module.
Crypto User	The Crypto User may perform general security functions as described in the Crypto-C ME Developer's Guide. The User may also call specific FIPS 140 module functions as defined in Crypto-C ME Developer's Guide.

4.4.1. Crypto Officer Role

An operator assuming the Crypto Officer role can call any of the module's functions. The complete list of the functionality available to the Crypto Officer is outlined in the Services section on page 13.

4.4.2. User Role

An operator assuming the Crypto User role can utilize the entire Crypto-C ME API except for the `CRYPTOC_FIPS140_me_fips140_self_test()` method, which is reserved for the Crypto Officer. The Crypto-C ME API functions are documented in the Services section on page 13.

4.5. Cryptographic Key Management

4.5.1. Key Generation

The Cryptographic Module supports generation of DSA, RSA, and Diffie-Hellman (DH) public and private keys. Furthermore, the module employs a FIPS 186-2 compliant random number generator for generating asymmetric and symmetric keys used in algorithms such as AES, DES, TDES, RSA, DSA or Diffie-Hellman.

4.5.2. Key Storage

Public and private keys are provided to the Cryptographic Module by the operator, and their state is destroyed when the operator indicates the key is finished being used. No persistent storage of keys is handled. The Cryptographic Module does not provide long-term cryptographic key storage. If an operator chooses to store keys, the operator is responsible for storing keys exported from the module.

4.5.3. Key Access

An authorized operator of the module has access to all key data created during the module's operation.

4.5.4. Key Protection/Zeroization

All key data resides in internally allocated data structures and can be output only using the module's defined API. The operating system protects memory and process space from unauthorized access. The operator should follow the steps outlined in the Cryptographic Module Developer's Guide to ensure sensitive data is protected by zeroizing the data from memory when it is no longer needed.

4.6. Cryptographic Algorithms

The Crypto-C ME module supports a wide variety of cryptographic algorithms. FIPS 140-2 requires that FIPS-approved algorithms be used whenever there is an applicable FIPS standard. The following table lists the FIPS approved algorithms supported by the Crypto-C ME module.

Table 2 - Crypto-C ME FIPS-approved algorithms

Algorithm	Validation Certificate
AES	Cert. 192
DES (For use in legacy systems only)	Cert. 278
3DES	Cert. 288
Diffie-Hellman	Non-Approved (Allowed in FIPS mode)
DSA	Cert. 121
FIPS 186-2 PRNG (Change Notice 1-with and without the mod q step)	Cert. 39
RSA X9.31 and PKCS#1	Cert. 29
RSA encrypt/decrypt	Non-Approved (Allowed in FIPS mode for key transport)
SHA-1	Cert. 272
SHA-256	Cert. 272
SHA-384	Cert. 272
SHA-512	Cert. 272
HMAC-SHA1	Cert. 7

Table 3 - Crypto-C ME Non-FIPS approved algorithms

Algorithm
MD2
MD5
HMAC MD5
DES40
RC2
RC4
RC5

For more information on using Crypto-C ME in a FIPS compliant manner refer to Secure Operation of the Cryptographic Module on page 11.

4.7. Self-Test

The Crypto-C ME module performs a number of power-up and conditional self-tests to ensure proper operation.

4.7.1. Power-Up Self-Tests

The power-up self-tests implemented in the Crypto-C ME module are:

- AES Known Answer Tests (KATs)
- TDES KATs
- DES KATs
- SHA-1 KATs
- SHA-256 KATs
- SHA-384 KATs
- SHA-512 KATs
- HMAC SHA-1 KATs
- RSA Sign/verify Test
- DSA Sign/verify Test
- PRNG KATs
- Software integrity test

Power-up self-tests are executed automatically when the module is loaded into memory.

4.7.2. Conditional Self-Tests

The Crypto-C ME module performs two conditional self-tests: a pair-wise consistency test each time the module generates a DSA, DH, or RSA public/private key pair, and a continuous random number generator test each time the module produces random data per its FIPS 186-2 random number generator.

4.7.3. Critical Functions Test

When operating in FIPS140_SSL_MODE, a known answer test is performed for MD5 and HMAC-MD5.

4.7.4. Mitigation of Other Attacks

RSA key operations implement blinding by default, providing a defense against timing attacks. Blinding is implemented through blinding modes, and the following options are available:

- Blinding mode off
- Blinding mode with no update, where the blinding value is constant for each operation
- Blinding mode with full update, where a new blinding value is used for each operation.

5. Secure Operation of the Cryptographic Module

This section provides an overview of how to securely operate the Crypto-C ME module in order to be in compliance with the FIPS140-2 standards.

5.1. Approved DSA and RSA Modulus Sizes

In the FIPS approved mode, the DSA key-pair modulus sizes should be between 512 and 1024 bits, and the RSA modulus size can range from 1024 to 4096 bits.

5.2. Operating the Cryptographic Module

The Cryptographic Module may be placed into FIPS mode by calling the `CRYPTOC_FIPS140_enable_FIPS140_operating_mode()` function. After making the `CRYPTOC_FIPS140_enable_FIPS140_operating_mode()` function call, the Cryptographic Module enforces that only the FIPS approved algorithms listed in the Services section on page 13 are available to operators. To disable FIPS mode, call CRYPTOC_FIPS140_enable_non_FIPS140_operating_mode().

The following Services are restricted to operation by the Crypto Officer:

- `CRYPTOC_FIPS140_me_fips140_self_test()`

The user of the Cryptographic Module shall link with the static library for their platform which will load the cryptographic module's shared library or dynamic link library at runtime. For additional details see the “FIPS 140-2 Library and Modes of Operation” section in the Crypto-C ME Developers Guide.

5.3. Modes of Operation

There are four modes of operation: `DISABLED_MODE, FIPS140_MODE, NON_FIPS140_MODE,` and `FIPS140_SSL_MODE`. Use the functions listed after each mode below to enter and to check that the module is in the specified mode.

Cryptographic keys must not be shared between FIPS140_MODE/FIPS140_SSL_MODE and DISABLED_MODE/NON_FIPS140_MODE.

5.3.1. DISABLED MODE

This mode indicates that the FIPS140 library is disabled, usually due to an internal or caller’s usage error. No future transition into `FIPS140_MODE` or `NON_FIPS140_MODE` is permitted. The caller’s current operating system process may continue to operate with the currently opened library and cryptographic contexts, but no additional contexts may be opened.

- `CRYPTOC_FIPS140_disable_operating_modes()`
- `CRYPTOC_FIPS140_operating_mode_is_disabled()`.

5.3.2. FIPS 140 MODE

This mode indicates that the FIPS140 library is running in `FIPS140_MODE`. A transition into `NON_FIPS140_MODE` shall only be made after all `FIPS140_MODE` library contexts have been closed.

- `CRYPTOC_FIPS140_enable_fips140_operating_mode()`
- `CRYPTOC_FIPS140_operating_mode_is_fips140()`.

5.3.3. NON FIPS 140 MODE

This mode indicates that the FIPS140 library is running in `NON_FIPS140_MODE`. A transition into `FIPS140_MODE` shall only be made after all `NON_FIPS140_MODE` library contexts have been closed.

- `CRYPTOC_FIPS140_enable_non_fips140_operating_mode()`
- `CRYPTOC_FIPS140_operating_mode_is_non_fips140()`.

5.3.4. FIPS 140 SSL MODE

This mode indicates that the FIPS140 library is running in `FIPS140_SSL_MODE`. A transition into `NON_FIPS140_MODE` shall only be made after all `FIPS140_SSL_MODE` library contexts have been closed.

`FIPS140_SSL_MODE` is `FIPS140_MODE` with the addition of those items required to perform TLS in a FIPS140-compatible manner.

- `CRYPTOC_FIPS140_enable_fips140_ssl_operating_mode()`
- `CRYPTOC_FIPS140_operating_mode_is_fips140_ssl()`.

6. Services

The Cryptographic Module provides the following services. For details of the operation of each of these services see the Developers Guide.

Table 4 - Crypto-C ME Services

Function	Function
BIO_append_filename	BIO_clear_flags
BIO_clear_retry_flags	BIO_copy_next_retry
BIO_debug_cb	BIO_dump
BIO_dump_format	BIO_dup_chain
BIO_f_buffer	BIO_f_null
BIO_find_type	BIO_flush
BIO_free	BIO_free_all
BIO_get_cb	BIO_get_cb_arg
BIO_get_close	BIO_get_flags
BIO_get_fp	BIO_get_retry_BIO
BIO_get_retry_reason	BIO_gets
BIO_method_name	BIO_method_type
BIO_new	BIO_new_file
BIO_new_fp	BIO_new_mem
BIO_open_file	BIO_pop
BIO_print_hex	BIO_printf
BIO_push	BIO_puts
BIO_read	BIO_read_filename
BIO_reference_inc	BIO_reset
BIO_rw_filename	BIO_s_file
BIO_s_mem	BIO_s_null
BIO_seek	BIO_set_bio_cb
BIO_set_cb	BIO_set_cb_arg
BIO_set_close	BIO_set_flags
BIO_set_fp	BIO_should_io_special
BIO_should_read	BIO_should_retry
BIO_should_write	BIO_tell
BIO_write	BIO_write_filename
CRYPTOC_FIPS140_disable_operating_modes	CRYPTOC_FIPS140_enable_fips140_operating_mode
CRYPTOC_FIPS140_enable_fips140_ssl_operating_mode	CRYPTOC_FIPS140_enable_non_fips140_operating_mode
CRYPTOC_FIPS140_get_mem_functions	CRYPTOC_FIPS140_get_self_test_result
CRYPTOC_FIPS140_get_startup_test_result	CRYPTOC_FIPS140_get_version
CRYPTOC_FIPS140_library_is_shared	CRYPTOC_FIPS140_lock_get_cb
CRYPTOC_FIPS140_lock_get_name	CRYPTOC_FIPS140_lock_num
CRYPTOC_FIPS140_lock_set_cb	CRYPTOC_FIPS140_me_fips140_self_test
CRYPTOC_FIPS140_me_fips140_startup_self_test	CRYPTOC_FIPS140_operating_mode_is_disabled
CRYPTOC_FIPS140_operating_mode_is_fips140	CRYPTOC_FIPS140_operating_mode_is_fips140_ssl
CRYPTOC_FIPS140_operating_mode_is_non_fips140	CRYPTOC_FIPS140_rand_get_default
CRYPTOC_FIPS140_rand_set_default	CRYPTOC_FIPS140_set_mem_functions
CRYPTOC_FIPS140_set_officer_sign_in_state	CRYPTOC_FIPS140_set_user_sign_in_state
CRYPTOC_FIPS140_sign_in_state_is_disabled	CRYPTOC_FIPS140_sign_in_state_is_officer
CRYPTOC_FIPS140_sign_in_state_is_user	CRYPTOC_ME_FIPS140_fips140_library_init
CRYPTOC_ME_FIPS140_library_free	CRYPTOC_ME_FIPS140_library_init

Function	Function
CRYPTOC_ME_FIPS140_library_set_info	CRYPTOC_ME_FIPS140_non_fips140_library_init
CRYPTOC_ME_get_default_resource_list	CRYPTOC_ME_get_small_resource_list
CRYPTOC_ME_library_free	CRYPTOC_ME_library_info
CRYPTOC_ME_library_info_type_from_string	CRYPTOC_ME_library_info_type_to_string
CRYPTOC_ME_library_new	CRYPTOC_ME_library_version
R_CR_asym_decrypt	R_CR_asym_decrypt_init
R_CR_asym_encrypt	R_CR_asym_encrypt_init
R_CR_CTX_alg_supported	R_CR_CTX_free
R_CR_CTX_get_info	R_CR_CTX_ids_from_sig_id
R_CR_CTX_ids_to_sig_id	R_CR_CTX_new
R_CR_CTX_set_info	R_CR_decrypt
R_CR_decrypt_final	R_CR_decrypt_init
R_CR_decrypt_update	R_CR_DEFINE_CUSTOM_CIPHER_LIST
R_CR_DEFINE_CUSTOM_METHOD_TABLE	R_CR_digest
R_CR_digest_final	R_CR_digest_init
R_CR_digest_update	R_CR_dup
R_CR_encrypt	R_CR_encrypt_final
R_CR_encrypt_init	R_CR_encrypt_update
R_CR_free	R_CR_generate_key
R_CR_generate_key_init	R_CR_generate_parameter
R_CR_generate_parameter_init	R_CR_get_default_imp_method
R_CR_get_default_method	R_CR_get_default_signature_map
R_CR_get_detail	R_CR_get_detail_string
R_CR_get_detail_string_table	R_CR_get_error
R_CR_get_error_string	R_CR_get_file
R_CR_get_function	R_CR_get_function_string
R_CR_get_function_string_table	R_CR_get_info
R_CR_get_line	R_CR_get_reason
R_CR_get_reason_string	R_CR_get_reason_string_table
R_CR_ID_from_string	R_CR_ID_to_string
R_CR_key_exchange_init	R_CR_key_exchange_phase_1
R_CR_key_exchange_phase_2	R_CR_mac
R_CR_mac_final	R_CR_mac_init
R_CR_mac_update	R_CR_new
R_CR_random_bytes	R_CR_random_seed
R_CR_RES_CRYPTO_CUSTOM_METHOD	R_CR_set_info
R_CR_sign	R_CR_sign_final
R_CR_sign_init	R_CR_sign_update
R_CR_SUB_from_string	R_CR_SUB_to_string
R_CR_TYPE_from_string	R_CR_TYPE_to_string
R_CR_verify	R_CR_verify_final
R_CR_verify_init	R_CR_verify_mac
R_CR_verify_mac_final	R_CR_verify_mac_init
R_CR_verify_mac_update	R_CR_verify_update
R_FORMAT_from_string	R_FORMAT_to_string
R_free	R_get_mem_functions
R_LIB_CTX_free	R_LIB_CTX_new
R_lock_ctrl	R_lock_get_cb
R_lock_get_name	R_lock_num
R_lock_r	R_lock_set_cb
R_lock_w	R_locked_add
R_locked_add_get_cb	R_locked_add_set_cb

Function	Function
R_lockid_new	R_lockids_free
R_malloc	R_PKEY_cmp
R_PKEY_CTX_free	R_PKEY_CTX_get_info
R_PKEY_CTX_get_LIB_CTX	R_PKEY_CTX_new
R_PKEY_CTX_set_info	R_PKEY_FORMAT_from_string
R_PKEY_FORMAT_to_string	R_PKEY_free
R_PKEY_from_binary	R_PKEY_from_bio
R_PKEY_from_file	R_PKEY_from_public_key_binary
R_PKEY_get_info	R_PKEY_get_num_bits
R_PKEY_get_num_primes	R_PKEY_get_PKEY_CTX
R_PKEY_get_type	R_PKEY_iterate_fields
R_PKEY_new	R_PKEY_pk_method
R_PKEY_print	R_PKEY_public_cmp
R_PKEY_reference_inc	R_PKEY_set_info
R_PKEY_to_binary	R_PKEY_to_bio
R_PKEY_to_public_key_binary	R_PKEY_TYPE_from_string
R_PKEY_TYPE_to_string	R_rand_add_entropy
R_rand_bytes	R_rand_entropy_count
R_rand_file_name	R_rand_free
R_rand_get_default	R_rand_get_entropy_func
R_rand_lib_cleanup	R_rand_load_file
R_rand_new	R_rand_seed
R_rand_set_default	R_rand_set_entropy_func
R_rand_write_file	R_realloc
R_remalloc	R_set_mem_functions
R_SKEY_free	R_SKEY_get_info
R_SKEY_new	R_SKEY_set_info
R_unlock_r	R_unlock_w

7. Acronyms/Definitions

The following table gives an explanation of the terms and acronyms used throughout this document.

Term	Description
AES	Advanced Encryption Standard. A fast block cipher with a 128-bit block, and keys of lengths 128, 192 and 256 bits. This will replace DES as the US symmetric encryption standard.
API	Application Programming Interface
Attack	Either a successful or unsuccessful attempt at breaking part or all of a cryptosystem. Various attack types include an algebraic attack, birthday attack, brute force attack, chosen ciphertext attack, chosen plaintext attack, differential cryptanalysis, known plaintext attack, linear cryptanalysis, and middleperson attack.
DES	Data Encryption Standard. A symmetric encryption algorithm with a 56-bit key. See also Triple DES.
Diffie-Hellman	The Diffie-Hellman asymmetric key exchange algorithm. There are many variants, but typically two entities exchange some public information (for example, public keys or random values) and combines them with their own private keys to generate a shared session key. As private keys are not transmitted, eavesdroppers are not privy to all of the information that composes the session key.
DSA	Digital Signature Algorithm. An asymmetric algorithm for creating digital signatures.
Encryption	The transformation of plaintext into an apparently less readable form (called ciphertext) through a mathematical process. The ciphertext may be read by anyone who has the key that decrypts (undoes the encryption) the ciphertext.
FIPS	Federal Information Processing Standards
HMAC	Keyed-Hashing for Message Authentication Code
Key	A string of bits used in cryptography, allowing people to encrypt and decrypt data. Can be used to perform other mathematical operations as well. Given a cipher, a key determines the mapping of the plaintext to the ciphertext. Various types of keys include: distributed key, private key, public key, secret key, session key, shared key, subkey, symmetric key, and weak key.
NIST	National Institute of Standards and Technology. A division of the US Department of Commerce (formerly known as the NBS) which produces security and cryptography-related standards.
OS	Operating System
PC	Personal Computer
PDA	Personal Digital Assistant
PPC	PowerPC
privacy	The state or quality of being secluded from the view and/or presence of others.
private key	The secret key in public key cryptography. Primarily used for decryption but also used for encryption with digital signatures.
PRNG	Pseudo Random Number Generator
RC2	Block cipher developed by Ron Rivest as an alternative to the DES. It has a block size of 64 bits and a variable key size. It is a legacy cipher and RC5 should be used in preference.
RC4	Symmetric algorithm designed by Ron Rivest using variable length keys (usually 40 bit or 128 bit).
RC5	Block cipher designed by Ron Rivest. It is parameterizable in its word size, key length and number of rounds. Typical use involves a block size of 64 bits, a key size of 128 bits and either 16 or 20 iterations of its round function.
RNG	Random Number Generator
RSA	Public key (asymmetric) algorithm providing the ability to encrypt data and create and verify digital signatures. RSA stands for Rivest, Shamir, and Adleman, the developers of the RSA public key cryptosystem.
SHA	Secure Hash Algorithm. An algorithm which creates a unique hash value for each possible input. SHA takes an arbitrary input which is hashed into a 160-bit digest.
SHA-1	A revision to SHA to correct a weakness. It produces 160-bit digests. SHA-1 takes an arbitrary input which is hashed into a 20-byte digest.
SHA-2	The NIST-mandated successor to SHA-1, to complement the Advanced Encryption Standard. It is a family of hash algorithms (SHA-256, SHA-384 and SHA-512) which produce digests of 256, 384 and 512 bits respectively.
Triple DES	A variant of DES which uses three 56-bit keys.

8. Contacting RSA Security

See the RSA Security Web site at http://www.rsasecurity.com for the latest news, security bulletins and information about coming events.

Go to http://www.rsasecurity.com/node.asp?id=1202 for RSA BSAFE product information.

The RSA Laboratories cryptography FAQ at http://www.rsasecurity.com/rsalabs/node.asp?id=2152 contains frequently asked questions.

RSA Developer Central at http://developer.rsasecurity.com enables you to interact with other developers and RSA Security staff, read security-related articles and get answers to security and product questions.

8.1. Support and Service

See http://www.rsasecurity.com./node.asp?id=1067 or https://knowledge.rsasecurity.com if you have any questions or require additional information.

8.2. Purchasing Printed Product Documentation

All documentation for your RSA Security product is included in electronic format on the CD or in the download you have received. You can print product documentation directly from these files if you require a hard copy.

RSA Security also offers customers the option to purchase printed and bound copies of key documents for some products. See http://www.rsasecurity.com/go/documentation for more information.

8.3. Feedback

We welcome your feedback on RSA Security documentation. Please e-mail bsafeuserdocs@rsasecurity.com.