

---

# **RSA BSAFE<sup>®</sup>** **Crypto-C**

**Cryptographic Components for C**

## **Library Reference Manual**

Version 4.2



**RSA Data Security.**

A Security Dynamics Company

---

## Copyright Notice

Copyright © 1994, 1996-1999 RSA Data Security, Inc. All rights reserved. This work contains proprietary information of RSA Data Security, Inc. Distribution is limited to authorized licensees of RSA Data Security, Inc. Any unauthorized reproduction or distribution of this document is strictly prohibited.

RSA is a trademark and BSAFE is a registered trademark of RSA Data Security, Inc.

The RSA Public Key Cryptosystem is protected by U.S. Patent #4,405,829.  
The RC5™ algorithm is protected by U.S. Patent #5,724,428 and #5,835,600.

The DES implementation in this product contains code based on the “libdes” package written by Eric A. Young (eay@mincom.oz.au) and is included with his permission.

---

# Contents

---

<b>Chapter 1</b>	<b>Introduction</b>	<b>1</b>
	Organization . . . . .	2
	The Crypto-C Environment . . . . .	3
	Memory Management . . . . .	4
	Code Example . . . . .	5
	The Algorithm Object . . . . .	8
	The Key Object . . . . .	9
	The Algorithm Chooser . . . . .	10
	The BDEMO Algorithm Chooser . . . . .	10
	Defining an Algorithm Chooser . . . . .	10
	The Surrender Function . . . . .	12
	Surrender . . . . .	13
	The ITEM Structure . . . . .	14
<b>Chapter 2</b>	<b>Algorithm Info Types</b>	<b>15</b>
	AI_BSSecretSharing . . . . .	17
	AI_CBC_IV8 . . . . .	19
	AI_DES_CBC_BSAFE1 . . . . .	20
	AI_DES_CBC_IV8 . . . . .	22
	AI_DES_CBCPadBER . . . . .	24
	AI_DES_CBCPadIV8 . . . . .	26
	AI_DES_CBCPadPEM . . . . .	28
	AI_DES_EDE3_CBC_IV8 . . . . .	30
	AI_DES_EDE3_CBCPadBER . . . . .	32
	AI_DES_EDE3_CBCPadIV8 . . . . .	34
	AI_DESX_CBC_BSAFE1 . . . . .	36
	AI_DESX_CBC_IV8 . . . . .	38
	AI_DESX_CBCPadBER . . . . .	40
	AI_DESX_CBCPadIV8 . . . . .	42
	AI_DHKeyAgree . . . . .	44

---

AI_DHKeyAgreeBER	46
AI_DHParamGen	48
AI_DSA	49
AI_DSASKeyGen	51
AI_DSAParamGen	53
AI_DSASWithSHA1	54
AI_DSASWithSHA1_BER	56
AI_ECAcceleratorTable	58
AI_ECBuildAcceleratorTable	59
AI_ECBuildPubKeyAccelTable	61
AI_EC_DHKeyAgree	63
AI_EC_DSA	65
AI_EC_DSASWithDigest	67
AI_EC_ES	69
AI_ECKKeyGen	70
AI_ECPParameters	72
AI_ECPParamGen	73
AI_ECPubKey	76
AI_FeedbackCipher	77
AI_HMAC	82
AI_HW_Random	84
AI_KeypairTokenGen	85
AI_MAC	87
AI_MD	88
AI_MD2	89
AI_MD2_BER	90
AI_MD2_PEM	92
AI_MD2Random	94
AI_MD2WithDES_CBCPad	95
AI_MD2WithDES_CBCPadBER	97
AI_MD2WithRC2_CBCPad	99
AI_MD2WithRC2_CBCPadBER	101
AI_MD2WithRSAEncryption	103
AI_MD2WithRSAEncryptionBER	105
AI_MD5	107
AI_MD5_BER	108
AI_MD5_PEM	110
AI_MD5Random	112
AI_MD5WithDES_CBCPad	113
AI_MD5WithDES_CBCPadBER	115
AI_MD5WithRC2_CBCPad	117

---

AI_MD5WithRC2_CBCPadBER . . . . .	119
AI_MD5WithRSAEncryption . . . . .	121
AI_MD5WithRSAEncryptionBER . . . . .	123
AI_MD5WithXOR . . . . .	125
AI_MD5WithXOR_BER . . . . .	127
AI_PKCS_OAEP_RSAPrivate . . . . .	129
AI_PKCS_OAEP_RSAPrivateBER . . . . .	133
AI_PKCS_OAEP_RSAPublic . . . . .	137
AI_PKCS_OAEP_RSAPublicBER . . . . .	141
AI_PKCS_OAEPRecode . . . . .	146
AI_PKCS_OAEPRecodeBER . . . . .	150
AI_PKCS_RSAPrivate . . . . .	155
AI_PKCS_RSAPrivateBER . . . . .	157
AI_PKCS_RSAPrivatePEM . . . . .	159
AI_PKCS_RSAPublic . . . . .	161
AI_PKCS_RSAPublicBER . . . . .	163
AI_PKCS_RSAPublicPEM . . . . .	165
AI_RC2_CBC . . . . .	167
AI_RC2_CBC_BSAFE1 . . . . .	169
AI_RC2_CBCPad . . . . .	171
AI_RC2_CBCPadBER . . . . .	173
AI_RC2_CBCPadPEM . . . . .	175
AI_RC4 . . . . .	177
AI_RC4_BER . . . . .	179
AI_RC4WithMAC . . . . .	181
AI_RC4WithMAC_BER . . . . .	183
AI_RC5_CBC . . . . .	185
AI_RC5_CBCPad . . . . .	187
AI_RC5_CBCPadBER . . . . .	189
AI_RESET_IV . . . . .	191
AI_RFC1113Recode . . . . .	192
AI_RSAKeyGen . . . . .	193
AI_RSAPrivate . . . . .	195
AI_RSAPrivateBSAFE1 . . . . .	197
AI_RSAPublic . . . . .	199
AI_RSAPublicBSAFE1 . . . . .	201
AI_RSAStrongKeyGen . . . . .	203
AI_SET_OAEP_RSAPrivate . . . . .	205
AI_SET_OAEP_RSAPublic . . . . .	207
AI_SHA1 . . . . .	209
AI_SHA1_BER . . . . .	210

AI_SHA1Random	212
AI_SHA1WithDES_CBCPad	213
AI_SHA1WithDES_CBCPadBER	215
AI_SHA1WithRSAEncryption	217
AI_SHA1WithRSAEncryptionBER	219
AI_SignVerify	221
AI_SymKeyTokenGen	223
AI_X931Random	225
AI_X962Random_V0	227

## Chapter 3 **Key Info Types** **229**

KI_8Byte	231
KI_24Byte	232
KI_DES8	233
KI_DES8Strong	234
KI_DES24Strong	235
KI_DES_BSAFE1	236
KI_DESX	237
KI_DESX_BSAFE1	238
KI_DSAPrivate	239
KI_DSAPrivateBER	241
KI_DSAPrivateX957BER	242
KI_DSAPublic	243
KI_DSAPublicBER	245
KI_DSAPublicX957BER	246
KI_ECPrivate	247
KI_ECPrivateComponent	248
KI_ECPublic	249
KI_ECPublicComponent	250
KI_ExtendedToken	251
KI_Item	253
KI_KeypairToken	254
KI_PKCS_RSAPrivate	256
KI_PKCS_RSAPrivateBER	257
KI_RC2_BSAFE1	258
KI_RC2WithBSAFE1Params	259
KI_RSA_CRT	260
KI_RSAPrivate	261
KI_RSAPrivateBSAFE1	263
KI_RSAPublic	264

KI_RSAPublicBER	265
KI_RSAPublicBSAFE1	266
KI-Token	267

---

**Chapter 4      Details of Crypto-C Functions      269**

B_BuildTableFinal	270
B_BuildTableGetBufSize	271
B_BuildTableInit	272
B_CreateAlgorithmObject	273
B_CreateKeyObject	274
B_CreateSessionChooser	275
B_DecodeDigestInfo	276
B_DecodeFinal	277
B_DecodeInit	278
B_DecodeUpdate	279
B_DecryptFinal	280
B_DecryptInit	281
B_DecryptUpdate	282
B_DestroyAlgorithmObject	283
B_DestroyKeyObject	284
B_DigestFinal	285
B_DigestInit	286
B_DigestUpdate	287
B_EncodeDigestInfo	288
B_EncodeFinal	289
B_EncodeInit	290
B_EncodeUpdate	291
B_EncryptFinal	292
B_EncryptInit	293
B_EncryptUpdate	294
B_FreeSessionChooser	295
B_GenerateInit	296
B_GenerateKeypair	297
B_GenerateParameters	298
B_GenerateRandomBytes	299
B_GetAlgorithmInfo	300
B_GetExtendedErrorInfo	301
B_GetKeyExtendedErrorInfo	302
B_GetKeyInfo	303
B_IntegerBits	304

---

B_KeyAgreeInit	305	
B_KeyAgreePhase1	306	
B_KeyAgreePhase2	307	
B_RandomInit	308	
B_RandomUpdate	309	
B_SetAlgorithmInfo	310	
B_SetKeyInfo	311	
B_SignFinal	312	
B_SignInit	313	
B_SignUpdate	314	
B_SymmetricKeyGenerate	315	
B_SymmetricKeyGenerateInit	316	
B_VerifyFinal	317	
B_VerifyInit	318	
B_VerifyUpdate	319	
T_free	320	
T_malloc	321	
T_memcmp	322	
T_memcpy	323	
T_memmove	324	
T_memset	325	
T_realloc	326	
T_strcmp	327	
T_strcpy	328	
T_strlen	329	
<b>Appendix A</b>	<b>Crypto-C Error Types</b>	<b>331</b>
<b>Appendix B</b>	<b>Platform-Specific Types and Constants</b>	<b>335</b>
	Types	335
	POINTER	335
	UINT2	335
	UINT4	336
	Constants	337
<b>Appendix C</b>	<b>References</b>	<b>339</b>

# Figures and Tables

## Figures

Figure 1-1	The Crypto-C environment . . . . .	3
Figure 2-1	Sample Algorithm Type . . . . .	16
Figure 3-1	Sample Key Info Type . . . . .	230

## Tables

Table 2-1	Algorithm methods for block ciphers. . . . .	78
Table 2-2	Algorithm methods for feedback modes . . . . .	79
Table A-1	Crypto-C Error Types . . . . .	329



# Introduction

---

This manual is a reference guide for developers who use RSA BSAFE® Crypto-C (Crypto-C), a core-cryptography SDK.

To familiarize yourself with Crypto-C, you may wish to read the *Crypto-C User's Manual* before referencing this manual. In particular, you may be interested in the “Introductory Example” in Chapter 1. The *User's Manual* also describes cryptographic concepts and shows how to successfully add Crypto-C to your application.

After you have read the *User's Manual* and understand the steps involved in creating a Crypto-C application, you can turn to this reference manual. The algorithm information types (AIs) carry the underlying cryptography, so we put this essential information up front (Chapter 2). Next, the key information types (KIs) provide the values for those AIs that require keys (Chapter 3). The last chapter (Chapter 4) contains the application programming interface (API) itself. Make sure to read this chapter, as it provides a review of the Crypto-C components.

---

# Organization

Chapter 1 introduces the components of the Crypto-C environment using a code example.

Chapters 2 and 3 are alphabetical listings of Crypto-C algorithm info types and key info types that specify the exact format of information supplied to and returned by Crypto-C.

Chapter 4 lists Crypto-C's functions alphabetically, giving full details of calling format and error return codes.

Appendix A lists Crypto-C error types.

Appendix B lists platform-specific types and constants.

Appendix C lists reference documents.

---

# The Crypto-C Environment

The typical Crypto-C environment consists of five components:

- an application
- an algorithm chooser
- a surrender function
- the Crypto-C SDK
- memory management routines

A Crypto-C component is specific to either an application or a platform, or it is part of the Crypto-C SDK (see Figure 1-1).

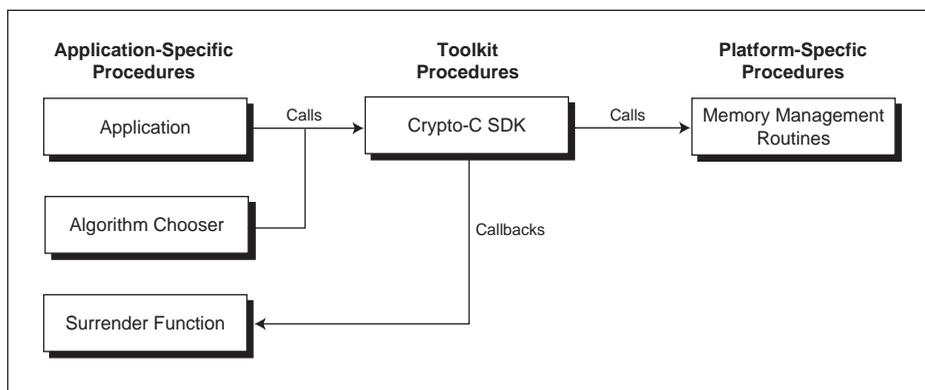


Figure 1-1 The Crypto-C environment

The application can be an encryption application, a key-generation application, or another similar application. The application calls Crypto-C and supplies the algorithm chooser and a callback to the surrender function. The algorithm chooser tells Crypto-C which method to use for a given algorithm. The surrender function allows processing or canceling during lengthy operations.

The Crypto-C SDK performs the cryptographic functions, such as encryption and key generation. The SDK is reentrant and suitable for shared or dynamic-link libraries.

---

# Memory Management

Crypto-C provides memory management routines that perform memory allocation (`T_malloc`, `T_realloc` and `T_free`) and memory operations (`T_memcmp`, `T_memcpy`, `T_memmove`, and `T_memset`). These functions are modeled after conventional C library functions such as `malloc`, `memset`, etc. If you want to use the Crypto-C memory-management functions, you must link in the `tstdlib.c` file when you build your application.

You can also supply your own versions of these functions if, for example, you need platform-specific routines. In this case, you link to your application both your memory-management functions and the Crypto-C library. Crypto-C will use these statically-linked functions in place of its memory management routines.

The BDEMO demonstration application provides a sample implementation of these functions. See “Details of Crypto-C Functions” on page 269 for descriptions and prototypes of these functions.

---

# Code Example

The following code example summarizes the six-step model used in Crypto-C. This model is described in depth in Chapter 1 of the *User's Manual*. The example encrypts data within a DES key, using a function named *EncryptData*. The inputs to *EncryptData* are: a pointer to the buffer, the data's length, a pointer to the 8-byte DES key value, and a pointer to the 8-byte initialization vector used by the DES-CBC algorithm. *EncryptData* writes the encrypted data to the buffer supplied by the caller and returns the length of the encrypted data.

```
#i ncl ude "agl obal . h"
#i ncl ude "bsafe. h"
#i ncl ude "demochos. h"
#defi ne NULL_SURRENDER_PTR ((A_SURRENDER_CTX *)NULL_PTR)

i nt EncryptData
    (output, outputLen, maxOutputLen, input, inputLen, keyValue, iv)
    unsigned char *output;                /* pointer to output data */
    unsigned int outputLen;                /* pointer to length of encrypted data */
    unsigned int maxOutputLen;            /* size of output buffer */
    unsigned char *input;                 /* pointer to input data buffer */
    unsigned int inputLen;                 /* length of input data */
    unsigned char *keyValue;              /* pointer to 8-byte DES key */
    unsigned char *iv;                    /* pointer to 8-byte initialization vector */

{
    B_ALGORI THM_OBJ desAl gori thm = (B_ALGORI THM_OBJ)NULL_PTR;
    B_KEY_OBJ desKey = (B_KEY_OBJ)NULL_PTR;
    B_BLK_CI PHER_W_FEEDBACK_PARAMS feedbackParams;
    I TEM ini tVector;
    unsigned int partOutLen;
    i nt status;

    /* break commands jump to the end of the do while (0) block */
    do {
        i f ((status = B_CreateKeyObj ect (&desKey)) != 0)
            break;
        i f ((status = B_SetKeyI nfo
            (desKey, KI_DES8Strong, (POI NTER)keyVal ue)) != 0)
            break;
    }
```

```

    if ((status = B_CreateAlgorithmObject (&desAlgorithm)) != 0)
        break;
    initVector.data = iv;
    initVector.len = 8;
    feedbackParams.encryptionMethodName = "des";
    feedbackParams.encryptionParams = NULL_PTR;
    feedbackParams.feedbackMethodName = "cbc";
    feedbackParams.feedbackParams = initVector;
    feedbackParams.paddingMethodName = "pad";
    feedbackParams.paddingParams = NULL_PTR;
    if ((status = B_SetAlgorithmInfo
        (desAlgorithm, (POINTER)&AI_FeedbackCipher,
        (POINTER)&feedbackParams)) != 0)
        break;

    if ((status = B_EncryptInit
        (desAlgorithm, desKey, DEMO_ALGORITHM_CHOOSER,
        NULL_SURRENDER_PTR)) != 0)
        break;
    if ((status = B_EncryptUpdate
        (desAlgorithm, output, outputLen, maxOutputLen, input,
        inputLen, (B_ALGORITHM_OBJ)NULL_PTR,
        NULL_SURRENDER_PTR)) != 0)
        break;

    if ((status = B_EncryptFinal
        (desAlgorithm, output + *outputLen, &partOutLen,
        maxOutputLen - *outputLen, (B_ALGORITHM_OBJ)NULL_PTR,
        NULL_SURRENDER_PTR)) != 0)
        break;
    *outputLen += partOutLen;
} while (0);

B_KEY_OBJ desKey = (B_KEY_OBJ)NULL_PTR;
B_ALGORITHM_OBJ desAlgorithm = (B_ALGORITHM_OBJ)NULL_PTR;
return (status);
}

```

The main work in *EncryptData* is done by the functions `B_EncryptInit`, `B_EncryptUpdate`, and `B_EncryptFinal`. The calling format for these and other functions is shown in Chapter 4, “Details of Crypto-C Functions.” Most Crypto-C procedures return either a zero for success or one of the error types listed in Appendix A.

---

*EncryptData* uses DEMO\_ALGORITHM\_CHOOSER as the *algorithmChooser* argument to B\_EncryptInit. The algorithm chooser is described on page 10. EncryptData also uses (A\_SURRENDER\_CTX \*)NULL\_PTR as the *surrenderContext* argument to B\_EncryptInit, B\_EncryptUpdate, and B\_EncryptFinal. As explained in Chapter 4, this tells Crypto-C to not call the surrender function. See the “The Surrender Function” on page 12 for an explanation of Crypto-C’s surrender routine.

---

# The Algorithm Object

In the above code example, `B_EncryptInit`, `B_EncryptUpdate`, and `B_EncryptFinal` use an *algorithm object* called *desAlgorithm*. An algorithm object holds information about an algorithm's parameters (for example, the DES initialization vector), and keeps a context during a cryptographic operation (for example, DES encryption).

Before Crypto-C can use an algorithm object, you must create and set it with `B_CreateAlgorithmObject` and `B_SetAlgorithmInfo`.

Every algorithm object that is created by `B_CreateAlgorithmObject` must be destroyed by `B_DestroyAlgorithmObject`. For security reasons, when Crypto-C destroys an algorithm object, it zeroes (in other words "zeros out" or sets to zero) and freezes any sensitive memory that the object allocated. Note that you can use an algorithm object for either encryption or decryption, but not for both. You must create separate algorithm objects to handle each case. Once you set an algorithm, do not reset it. In other words, once you call `B_SetAlgorithmInfo` for a particular algorithm object, do not call it again for the same object until that object has been destroyed and recreated.

As shown in Chapter 4, page 310, `B_SetAlgorithmInfo` has three input arguments, *algorithmObject*, *infoType*, and *info*. *algorithmObject* is the name of the algorithm object you are setting. *infoType* is one of the algorithm info types (AIs) listed in Chapter 2. The AI specifies which algorithm to use, such as DES-CBC, as well as the format of the actual algorithm information supplied by *info*.

As shown in Chapter 2, page 77, the format of *info* supplied to `B_SetAlgorithmInfo` for `AI_FeedbackCipher` is a pointer to a `B_BLK_CIPHER_W_FEEDBACK_PARAMS` structure that holds the necessary information for the encryption object. This data includes the encryption method name ("des"), the feedback method name ("cbc"), and a pointer to an `ITEM` structure that contains the 8 bytes of the initialization vector (*iv*), which seeds the process. In the example above, the data in the `ITEM` structure is the *iv* input argument to *EncryptData*.

---

# The Key Object

In the above code example, `B_EncryptInit` uses a *key object* called *desKey*. A key object holds a key's value, such as the DES key, and supplies this value to a function such as `B_EncryptInit`, that needs a key. A key object also receives the output of key generation such as `B_GenerateKeypair`.

Before Crypto-C can use a key object, you must create and set it with `B_CreateKeyObject` and `B_SetKeyInfo`. Every key object created by `B_CreateKeyObject` must be destroyed by `B_DestroyKeyObject`. For security reasons, when Crypto-C destroys a key object, it zeroizes (in other words, “zeros out” or sets to zero) and freezes any sensitive memory that the object allocated. Once you call `B_SetKeyInfo` for a particular key object, do not call it again for the same object until it has been destroyed and recreated.

As shown in Chapter 4, page 311, `B_SetKeyInfo` has two input arguments, *infoType* and *info*. *infoType* is one of the KI key info types listed in Chapter 3. The key info type specifies the format of the actual key information supplied by *info*.

As shown in Chapter 3, the format of *info* supplied to `B_SetKeyInfo` for `KI_DES8Strong` is a pointer to an unsigned char array that holds the 8-byte DES key. In the example, this is the *keyValue* input argument to `EncryptData`.

# The Algorithm Chooser

The algorithm chooser lists all the algorithm methods that Crypto-C will use in the application. In this way, you only link in the code you need, and thereby reduce the executable size.

## The BDEMO Algorithm Chooser

The BDEMO demonstration application supplied with Crypto-C defines an algorithm chooser called `DEMO_ALGORITHM_CHOOSER`. To use the BDEMO algorithm chooser, compile and link the module that defines `DEMO_ALGORITHM_CHOOSER` (as it is done for BDEMO) and specify `DEMO_ALGORITHM_CHOOSER` as the *algorithmChooser* argument.

## Defining an Algorithm Chooser

The main reason for an application to define its own algorithm chooser is to make the executable image smaller. The linker links in the object code for all algorithm methods listed in the algorithm chooser. To illustrate, an application that only uses MD5 and DES-CBC may define an algorithm chooser with only the MD5 and DES-CBC methods. In this way, the linker will only link in the object code related to MD5 and DES-CBC.

An algorithm chooser is an array of pointers to `B_ALGORITHM_METHOD` values. The last element of the array must be `(B_ALGORITHM_METHOD *)NULL_PTR`. The following is an example that defines an algorithm chooser called `MD5_DES_CBC_CHOOSER` for the MD5 and DES-CBC algorithm methods needed when using the `AI_MD5withDES_CBCPad` AI algorithm info type:

```
B_ALGORITHM_METHOD *MD5_DES_CBC_CHOOSER[] = {
    &AM_MD5,
    &AM_DES_CBC_ENCRYPT,
    &AM_DES_CBC_DECRYPT,
    (B_ALGORITHM_METHOD *)NULL_PTR
};
```

For additional examples of algorithm choosers, see “Algorithm Choosers” on page 118 of the *User’s Manual*.

Notice that encryption/decryption algorithm methods (AMs) such as DES-CBC, have separate entries for encryption and decryption. This separation of methods enables a

minimal footprint. If an application only performs encryption, it may use an algorithm chooser with only the encrypt method to prevent the linker from linking in the object code for decryption.

**Note:** Early versions of Crypto-C offered optimized AMs for some algorithms on selected platforms. For instance, when employing RSA public encryption, there were: `AM_RSA_ENCRYPT`, `AM_RSA_ENCRYPT_68` for the MPW compiler on 68K machines, and `AM_RSA_ENCRYPT_86` for the Microsoft compiler on x86 platforms. In versions 3.0 and higher, the optimized code for a particular algorithm, when available, is automatically linked in with the standard AM. So while it is no longer necessary to specify an optimized AM to link in optimized code, the old AM-specific optimized code is still valid.

## The Surrender Function

During lengthy operations, such as public-key computations and key generation, Crypto-C surrenders control to the application's surrender function. The surrender function may notify users of the operation being performed, indicate that it is still performing, process operating system tasks, or execute other operations before returning to Crypto-C. The surrender function may also cause Crypto-C to cancel the operation by returning a non-zero value.

Your application specifies its surrender function through an `A_SURRENDER_CTX` value. `A_SURRENDER_CTX` is supplied as the *surrenderContext* argument to Crypto-C functions such as `B_EncryptInit`. `A_SURRENDER_CTX` is defined as follows:

```
typedef struct {
    int (*Surrender) ( );           /* surrender function callback */
    POINTER handle;              /* application-specific information */
    POINTER reserved;            /* reserved for future use */
} A_SURRENDER_CTX;
```

An `A_SURRENDER_CTX` value consists of a pointer to your application-specific callback function (that constitutes Crypto-C's surrender function) and a pointer to application-specific information. The pointer to application-specific information is supplied directly to your callback and is not otherwise manipulated by Crypto-C. The reserved value should be set to `NULL_PTR` for future compatibility.

A typical application initializes the `A_SURRENDER_CTX` value before calling a Crypto-C procedure. Each `A_SURRENDER_CTX` value may specify a different surrender function callback and a different handle.

For a sample surrender function, see "A Sample Surrender Function" on page 121 of the *User's Manual*.

## Surrender

The surrender function callback must have the following form:

```
int (*Surrender) (  
    POINTER handle                /* application-specific information */  
);
```

*Surrender* is a developer-supplied function that actually performs the tasks required by the application. *handle* is the application-specific handle from the surrender context.

*Surrender* should return 0 for Crypto-C to continue its operation, or a non-zero value for Crypto-C to cancel its operation.

### Return value

0	continue with operation
non-zero	cancel operation

## The ITEM Structure

Often, Crypto-C requires that input be in the form of an ITEM structure, defined as follows:

```
typedef struct {  
    unsigned char *data;  
    unsigned int   len;  
} ITEM;
```

# Algorithm Info Types

---

This chapter lists the standard algorithm info types (AIs) offered in RSA BSAFE Crypto-C (Crypto-C). A typical application supplies an algorithm info type as the *infoType* argument to `B_SetAlgorithmInfo`. For examples of how to use algorithm info types with certain algorithms, see the *User's Manual*.

An AI not only specifies which algorithm to use, but also specifies the format of the algorithm parameters. You supply the algorithm parameters as the *info* argument to `B_SetAlgorithmInfo`.

The entry for each AI occupies one or two pages. See the next page for a description of the entry format.

Some algorithm info types, such as encryption and signature algorithms, need a key object. If an algorithm calls for a key object, the AI entry will describe which KI to use to set the key object. For a complete list of KIs, see Chapter 3.

The algorithm info types pass information from and to various `B_` functions. See Chapter 4 for the descriptions and prototypes of these functions.

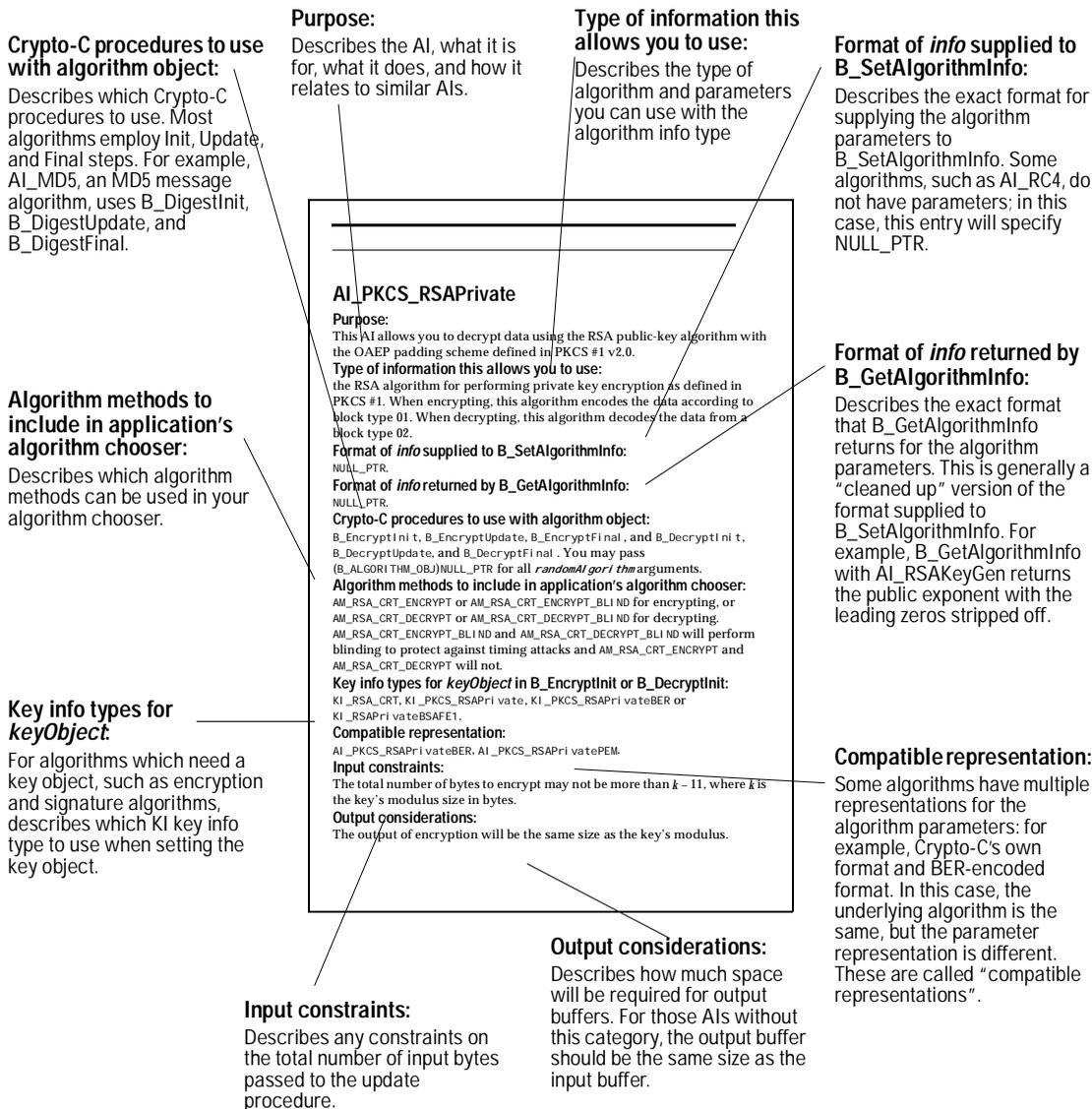


Figure 2-1 Sample Algorithm Type

## AI\_BSSecretSharing

### Purpose:

This AI allows you to split a highly sensitive secret, such as a private key, into several "shares", which can be reassembled to recreate the original secret. The secret can only be recreated if there are at least a "threshold" number of shares present. For example, the secret can be divided into five shares. If the threshold is three, any three of them can be used to reconstruct the secret.

### Type of information this allows you to use:

the Bloom-Shamir secret sharing algorithm as defined in "Generalized Linear Threshold Scheme" by S.C. Kothari, *Proceedings of CRYPTO 84*.

### Format of *info* supplied to B\_SetAlgorithmInfo:

pointer to a B\_SECRET\_SHARING\_PARAMS structure:

```
typedef struct {
    unsigned int threshold;           /* share threshold */
} B_SECRET_SHARING_PARAMS;
```

The *threshold* is the minimum number of shares required to recover the secret key; it has a minimum value of 2 and maximum of 255.

### Format of *info* returned by B\_GetAlgorithmInfo:

pointer to a B\_SECRET\_SHARING\_PARAMS structure (see above).

### Crypto-C procedures to use with algorithm object:

B\_EncryptInit, B\_EncryptUpdate, B\_EncryptFinal, B\_DecryptInit, B\_DecryptUpdate, and B\_DecryptFinal.

B\_EncryptUpdate must be called a minimum of *threshold* times. Each time, the secret being split must be supplied as the input and one new share is returned as the output. B\_EncryptFinal returns a status of BE\_OUTPUT\_COUNT if the number of calls to B\_EncryptUpdate calls is less than the *threshold*. B\_EncryptFinal supplies no output.

You must supply an initialized random algorithm to B\_EncryptUpdate. (The random

algorithm is used only on the first call to `B_EncryptUpdate`). Supply `(B_ALGORITHM_OBJ) NULL_PTR` as the *randomAlgorithm* for `B_EncryptFinal`.

`B_DecryptUpdate` must be called *threshold* times to supply enough shares to recover the secret key. `B_DecryptFinal` returns a status of `BE_INPUT_COUNT` if the number of calls to `B_DecryptUpdate` is less than the *threshold*, otherwise, it returns a success status and outputs the secret key.

Supply `(B_ALGORITHM_OBJ) NULL_PTR` as the *randomAlgorithm* for `B_DecryptUpdate` and `B_DecryptFinal`. Supply `(B_KEY_OBJ) NULL_PTR` as the *keyObject* for `B_EncryptInit` and `B_DecryptInit`.

### Output considerations:

The size of the output from each call to `B_EncryptUpdate` will be one byte more than the size of the secret. That byte represents the share.

## AI\_CBC\_IV8

### Purpose:

This AI allows you to change the initialization vector (IV) for a CBC-mode cipher without the need to create a new algorithm object or bind in a new key. This increases the performance of applications that have a long-lived symmetric key (e.g., DES key) used to encrypt many blocks or messages, each with a unique IV.

### Type of information this allows you to use:

a new 8-byte initialization vector for an existing CBC algorithm object previously initialized with one of the following AIs:

AI\_DES\_CBC\_IV8, AI\_DES\_CBCPad\_IV8, AI\_DES\_CBCPadBER, AI\_DES\_CBCPadPEM, AI\_DES\_EDE3\_CBC\_IV8, AI\_DES\_EDE3\_CBCPad\_IV8, AI\_DES\_EDE3\_CBCPadBER, AI\_DESX\_CBC\_IV8, AI\_DESX\_CBCPad\_IV8, AI\_DESX\_CBCPadBER, AI\_RC2\_CBC, AI\_RC2\_CBCPad, AI\_RC2\_CBCPadBER, AI\_RC2\_CBCPadPEM, AI\_RC5\_CBC, and AI\_RC5\_CBCPad.

### Format of *info* supplied to B\_SetAlgorithmInfo:

pointer to an 8-byte unsigned char array containing the new initialization vector.

This new initialization vector will not affect the current algorithm object until the next call to B\_EncryptInit, B\_EncryptFinal, B\_DecryptInit, or B\_DecryptFinal.

After the new IV takes effect on the algorithm object, any results from a previous call to B\_GetAlgorithmInfo on the algorithm object are undefined.

### Format of *info* returned by B\_GetAlgorithmInfo:

B\_GetAlgorithmInfo is not supported for AI\_CBC\_IV8.

### Crypto-C procedures to use with algorithm object:

B\_SetAlgorithmInfo.

## AI\_DES\_CBC\_BSAFE1

### Purpose:

Deprecated. This AI is included only for backward compatibility.

### Type of information this allows you to use:

the encryption type parameter (pad, pad with checksum, or raw) for the DES encryption algorithm as defined by BSAFE 1.x.

### Format of *info* supplied to `B_SetAlgorithmInfo`:

pointer to a `B_BSAFE1_ENCRYPTI ON_PARAMS` structure:

```
typedef struct {  
    int encrypti onType; /* encryption type */  
} B_BSAFE1_ENCRYPTI ON_PARAMS;
```

*encrypti onType* should be set to `B_BSAFE1_PAD` for pad mode, `B_BSAFE1_PAD_CHECKSUM` for pad with checksum mode, or `B_BSAFE1_RAW` for raw mode.

### Format of *info* returned by `B_GetAlgorithmInfo`:

pointer to a `B_BSAFE1_ENCRYPTI ON_PARAMS` structure (see above).

### Crypto-C procedures to use with algorithm object:

`B_EncryptI nit`, `B_EncryptUpdate`, `B_EncryptFi nal`, `B_DecryptI nit`, `B_DecryptUpdate`, and `B_DecryptFi nal`. You may pass `(B_ALGORI THM_OB J) NULL_PTR` for all *randomAl gori thm* arguments.

### Algorithm methods to include in application's algorithm chooser:

`AM_DES_CBC_ENCRYPT` for encryption and `AM_DES_CBC_DECRYPT` for decryption.

### Key info types for *keyObject* in `B_EncryptI nit` or `B_DecryptI nit`:

`KI_DES8Strong`, `KI_DES8`, `KI_8Byte`, or `KI_I tem` (if the length of the `I TEM` is 8).

**Input constraints:**

During encryption, this algorithm does not pad the output. Thus, you must provide input that is a multiple of 8 bytes.

**Output considerations:**

In pad mode, the total number of output bytes from encryption can be as many as 8 bytes more than the total input. In pad with checksum mode, the total number of output encryption bytes can be as many as 16 bytes more than the total input.

## AI\_DES\_CBC\_IV8

### Purpose:

This AI allows you to perform DES encryption or decryption in CBC mode with an 8-byte initialization vector on data that is a multiple of 8 bytes long. No padding will be performed. See AI\_DES\_CBCPadI V8 for the same algorithm type with padding.

### Type of information this allows you to use:

an 8-byte initialization vector for the DES-CBC encryption algorithm as defined in FIPS PUB 46-1 and FIPS PUB 81.

### Format of *info* supplied to B\_SetAlgorithmInfo:

pointer to an unsigned char array that holds the 8 bytes of the initialization vector.

### Format of *info* returned by B\_GetAlgorithmInfo:

pointer to an unsigned char array that holds the 8 bytes of the initialization vector.

### Crypto-C procedures to use with algorithm object:

B\_EncryptInit, B\_EncryptUpdate, B\_EncryptFinal, B\_DecryptInit, B\_DecryptUpdate, and B\_DecryptFinal. You may pass (B\_ALGORITHM\_OBJ)NULL\_PTR for all *randomAlgorithm* arguments.

### Algorithm methods to include in application's algorithm chooser:

AM\_DES\_CBC\_ENCRYPT for encryption and AM\_DES\_CBC\_DECRYPT for decryption.

### Key info types for *keyObject* in B\_EncryptInit or B\_DecryptInit:

KI\_DES8Strong, KI\_DES8, KI\_8Byte, KI\_Item (if the length of the ITEM is 8), or KI\_DES\_BSAFE1.

### Input constraints:

During encryption, this algorithm does not pad the output. Thus, you must provide input that is a multiple of 8 bytes.

## Token-based algorithm methods:



AI\_DES\_CBC\_IV8 can be used to access the hardware-related algorithm methods AM\_TOKEN\_DES\_CBC\_ENCRYPT and AM\_TOKEN\_DES\_CBC\_DECRYPT, for use in conjunction with BHAPI.

## Token-based key info types:

When used with one of the hardware algorithm methods described, AI\_DES\_CBC\_IV8 should be used with KI\_Token or KI\_ExtendedToken.

## AI\_DES\_CBCPadBER

### Purpose:

This AI is similar to AI\_DES\_CBCPadV8 except that it uses the ASN.1 BER format. This AI allows you to parse and create ASN.1 algorithm identifiers such as those used in PKCS #7 and other protocols. You call B\_SetAlgorithmInfo to initialize an algorithm object from the encoded algorithm identifier, which includes the initialization vector. Alternatively, you call B\_GetAlgorithmInfo with this AI to create an encoded algorithm identifier from an algorithm object created with AI\_DES\_CBCPadBER, AI\_DES\_CBCPadV8, or AI\_DES\_CBCPadPEM. The OID for this algorithm—excluding the tag and length bytes—in decimal, is "43, 14, 3, 2, 7". Also see AI\_DES\_CBCPadV8.

### Type of information this allows you to use:

the encoded algorithm identifier that specifies the DES-CBC With Padding encryption algorithm as defined in FIPS PUB 46-1 and FIPS PUB 81, with padding scheme defined in PKCS #5 and desCBC algorithm identifier defined in [NIST91].

### Format of *info* supplied to B\_SetAlgorithmInfo:

pointer to an ITEM structure that gives the address and length of the BER-encoded algorithm identifier. The encoding is converted to DER before it is copied to the algorithm object. B\_SetAlgorithmInfo returns BE\_WRONG\_ALGORITHM\_INFO if the algorithm identifier specifies an algorithm other than DES-CBC With Padding.

### Format of *info* returned by B\_GetAlgorithmInfo:

pointer to an ITEM structure that gives the address and length of the DER-encoded algorithm identifier.

### Crypto-C procedures to use with algorithm object:

B\_EncryptInit, B\_EncryptUpdate, B\_EncryptFinal, B\_DecryptInit, B\_DecryptUpdate, and B\_DecryptFinal. You may pass (B\_ALGORITHM\_OBJ)NULL\_PTR for all *randomAlgorithm* arguments.

### Algorithm methods to include in application's algorithm chooser:

AM\_DES\_CBC\_ENCRYPT for encryption and AM\_DES\_CBC\_DECRYPT for decryption.

## Key info types for *keyObject* in B\_EncryptInit or B\_DecryptInit:

KI\_DES8Strong, KI\_DES8, KI\_8Byte, KI\_Item (if the length of the ITEM is 8), or KI\_DES\_BSAFE1.

## Compatible representation:

AI\_DES\_CBCPadIV8, AI\_DES\_CBCPadPEM.

## Output considerations:

During encryption, this AI pads the output (which DES requires to be a multiple of 8 bytes long). Thus, the total number of output bytes from encryption can be as many as 8 bytes more than the total output.

## AI\_DES\_CBCPadIV8

### Purpose:

This AI allows you to perform DES encryption or decryption in CBC mode with an 8-byte initialization vector on data that is of any byte length. The padding mode is PKCS #5, which makes the ciphertext 1 to 8 bytes longer than the plaintext. See AI\_DES\_CBC\_IV8 for the same algorithm type with no padding. See AI\_DES\_CBCPadBER for the same algorithm type with BER encoding.

### Type of information this allows you to use:

an 8-byte initialization vector for the DES-CBC With Padding encryption algorithm as defined in FIPS PUB 46-1 and FIPS PUB 81, with padding scheme defined in PKCS #5.

### Format of *info* supplied to B\_SetAlgorithmInfo:

pointer to an unsigned char array that holds the 8 bytes of the initialization vector.

### Format of *info* returned by B\_GetAlgorithmInfo:

pointer to an unsigned char array that holds the 8 bytes of the initialization vector.

### Crypto-C procedures to use with algorithm object:

B\_EncryptInit, B\_EncryptUpdate, B\_EncryptFinal, B\_DecryptInit, B\_DecryptUpdate, and B\_DecryptFinal. You may pass (B\_ALGORITHM\_OBJ)NULL\_PTR for all *randomAlgorithm* arguments.

### Algorithm methods to include in application's algorithm chooser:

AM\_DES\_CBC\_ENCRYPT for encryption and AM\_DES\_CBC\_DECRYPT for decryption.

### Key info types for *keyObject* in B\_EncryptInit or B\_DecryptInit:

KI\_DES8Strong, KI\_DES8, KI\_8Byte, KI\_Item (if the length of the ITEM is 8), or KI\_DES\_BSAFE1.

### Compatible representation:

AI\_DES\_CBCPadBER, AI\_DES\_CBCPadPEM.

## Output considerations:

During encryption, this AI pads the output (which DES requires to be a multiple of 8 bytes long). Thus, the total number of output bytes from encryption can be as many as 8 bytes more than the total output.

## AI\_DES\_CBCPadPEM

### Purpose:

This AI is similar to AI\_DES\_CBCPadV8 except that it uses the format defined in the Privacy Enhanced Mail protocol (PEM). This AI allows you to parse and create PEM algorithm identifiers. First, you call B\_SetAlgorithmInfo to initialize an algorithm object from the encoded algorithm identifier that includes the initialization vector. Alternatively, you call B\_GetAlgorithmInfo with this AI to create an encoded algorithm identifier from an algorithm object created using AI\_DES\_CBCPadPEM, AI\_DES\_CBCPadV8 or AI\_DES\_CBCPadBER. Also see AI\_DES\_CBCPadV8.

### Type of information this allows you to use:

an RFC 1423 identifier that specifies the DES-CBC With Padding encryption algorithm as defined in FIPS PUB 46-1 and FIPS PUB 81, with padding scheme defined in RFC 1423. This algorithm info type is intended to process the value of a DEK-Info field in a PEM encapsulated header.

### Format of *info* supplied to B\_SetAlgorithmInfo:

pointer to a null-terminated string (char \*) that gives the DES-CBC identifier and 8-byte initialization vector, for example, "DES-CBC, 0123456789ABCDEF". Space and tab characters are removed from the string before it is copied to the algorithm object. B\_SetAlgorithmInfo returns BE\_WRONG\_ALGORITHM\_INFO if the algorithm identifier specifies an identifier other than DES-CBC.

### Format of *info* returned by B\_GetAlgorithmInfo:

pointer to a null-terminated string that gives the DES-CBC identifier and 8-byte initialization vector.

### Crypto-C procedures to use with algorithm object:

B\_EncryptInit, B\_EncryptUpdate, B\_EncryptFinal, B\_DecryptInit, B\_DecryptUpdate, and B\_DecryptFinal. You may pass (B\_ALGORITHM\_OBJ)NULL\_PTR for all *randomAlgorithm* arguments.

### Algorithm methods to include in application's algorithm chooser:

AM\_DES\_CBC\_ENCRYPT for encryption and AM\_DES\_CBC\_DECRYPT for decryption.

**Key info types for *keyObject* in B\_EncryptInit or B\_DecryptInit:**

KI\_DES8Strong, KI\_DES8, KI\_8Byte, KI\_Item (if the length of the ITEM is 8) or KI\_DES\_BSAFE1.

**Compatible representation:**

AI\_DES\_CBCPadIV8, AI\_DES\_CBCPadBER.

**Output considerations:**

During encryption, this AI pads the output (which DES requires to be a multiple of 8 bytes long). Thus, the total number of output bytes from encryption can be as many as 8 bytes more than the total output.

## AI\_DES\_EDE3\_CBC\_IV8

### Purpose:

This AI allows you to perform three-key DES in encrypt-decrypt-encrypt mode as defined in ANSI X9.17 using the outer-CBC mode. This AI is initialized with an 8-byte IV and operates on data that is an exact multiple of 8 bytes long. No padding will be performed. See AI\_DES\_EDE3\_CBCPadIV8 for the same algorithm type with padding.

### Type of information this allows you to use:

an 8-byte initialization vector for the DES-EDE3-CBC encryption algorithm.

### Format of *info* supplied to B\_SetAlgorithmInfo:

pointer to an unsigned char array that holds the 8 bytes of the initialization vector.

### Format of *info* returned by B\_GetAlgorithmInfo:

pointer to an unsigned char array that holds the 8 bytes of the initialization vector.

### Crypto-C procedures to use with algorithm object:

B\_EncryptInit, B\_EncryptUpdate, B\_EncryptFinal, B\_DecryptInit, B\_DecryptUpdate, and B\_DecryptFinal. You may pass (B\_ALGORITHM\_OBJ)NULL\_PTR for all *randomAlgorithm* arguments.

### Algorithm methods to include in application's algorithm chooser:

AM\_DES\_EDE3\_CBC\_ENCRYPT for encryption and AM\_DES\_EDE3\_CBC\_DECRYPT for decryption.

### Key info types for *keyObject* in B\_EncryptInit or B\_DecryptInit:

KI\_DES24Strong, KI\_24Byte, or KI\_Item (if the length of the ITEM is 24).

### Input constraints:

During encryption, this algorithm does not pad the output. Thus, you must provide input that is a multiple of 8 bytes.

## Token-based algorithm methods:



AI\_DES\_EDE3\_CBC\_IV8 may be used to access the hardware-related algorithm methods AM\_TOKEN\_DES\_EDE3\_CBC\_ENCRYPT and AM\_TOKEN\_DES\_EDE3\_CBC\_DECRYPT, for use with BHAPI.

## Token-based key info types:

When used with one of the hardware algorithm methods listed above, AI\_DES\_EDE3\_CBC\_IV8 should be used with KI\_Token or KI\_ExtendedToken.

## AI\_DES\_EDE3\_CBCPadBER

### Purpose:

This AI is similar to AI\_DES\_EDE3\_CBCPadIV8 except that it uses the ASN.1 BER format. This AI allows you to parse and create ASN.1 algorithm identifiers such as used in PKCS #7 and other protocols. You call B\_SetAlgorithmInfo to initialize an algorithm object from the encoded algorithm identifier that includes the initialization vector. You call B\_GetAlgorithmInfo with this AI to create an encoded algorithm identifier from an algorithm object that was created using AI\_DES\_EDE3\_CBC\_PadIV8 or AI\_DES\_EDE3\_CBCPadBER. The OID for this algorithm, excluding the tag and length bytes, in decimal, is "42, 134, 72, 134, 247, 13, 3, 7". Also see AI\_DES\_EDE3\_CBCPadIV8.

### Type of information this allows you to use:

the encoding of an algorithm identifier that specifies the DES-EDE3-CBC encryption algorithm, with padding scheme defined in PKCS #5.

### Format of *info* supplied to B\_SetAlgorithmInfo:

pointer to an ITEM structure that gives the address and length of the BER-encoded algorithm identifier. The encoding is converted to DER before it is copied to the algorithm object. B\_SetAlgorithmInfo returns BE\_WRONG\_ALGORITHM\_INFO if the algorithm identifier specifies an algorithm other than DES-EDE3-CBC With Padding.

### Format of *info* returned by B\_GetAlgorithmInfo:

pointer to an ITEM structure that gives the address and length of the DER-encoded algorithm identifier.

### Crypto-C procedures to use with algorithm object:

B\_EncryptInit, B\_EncryptUpdate, B\_EncryptFinal, B\_DecryptInit, B\_DecryptUpdate, and B\_DecryptFinal. You may pass (B\_ALGORITHM\_OBJ)NULL\_PTR for all *randomAlgorithm* arguments.

## Algorithm methods to include in application's algorithm chooser:

AM\_DES\_EDE3\_CBC\_ENCRYPT for encryption and AM\_DES\_EDE3\_CBC\_DECRYPT for decryption.

## Key info types for *keyObject* in B\_EncryptInit or B\_DecryptInit:

KI\_DES24Strong, KI\_24Byte, or KI\_Item (if the length of the ITEM is 24).

## Compatible representation:

AI\_DES\_EDE3\_CBCPadV8.

## Output considerations:

During encryption, this AI pads the output (which DES requires to be a multiple of 8 bytes long). Thus, the total number of output bytes from encryption can be as many as 8 bytes more than the total output.

## AI\_DES\_EDE3\_CBCPadIV8

### Purpose:

This AI allows you to perform three-key DES in encrypt-decrypt-encrypt mode as defined in ANSI X9.17 using the outer-CBC mode. This AI is initialized with an 8-byte IV and operates on data that is of any byte length. The padding mode is PKCS #5, which makes the ciphertext 1 to 8 bytes longer than the plaintext. See `AI_DES_EDE3_CBC_IV8` for the same algorithm type with no padding. See `AI_DES_EDE3_CBCPadBER` for the same algorithm type with BER encoding.

### Type of information this allows you to use:

an 8-byte initialization vector for the DES-EDE3-CBC encryption algorithm, with padding scheme defined in PKCS #5.

### Format of *info* supplied to `B_SetAlgorithmInfo`:

pointer to an unsigned char array that holds the 8 bytes of the initialization vector.

### Format of *info* returned by `B_GetAlgorithmInfo`:

pointer to an unsigned char array that holds the 8 bytes of the initialization vector.

### Crypto-C procedures to use with algorithm object:

`B_EncryptInit`, `B_EncryptUpdate`, `B_EncryptFinal`, `B_DecryptInit`, `B_DecryptUpdate`, and `B_DecryptFinal`. You may pass `(B_ALGORITHM_OBJ)NULL_PTR` for all *randomAlgorithm* arguments.

### Algorithm methods to include in application's algorithm chooser:

`AM_DES_EDE3_CBC_ENCRYPT` for encryption and `AM_DES_EDE3_CBC_DECRYPT` for decryption.

### Key info types for *keyObject* in `B_EncryptInit` or `B_DecryptInit`:

`KI_DES24Strong`, `KI_24Byte`, or `KI_Item` (if the length of the `ITEM` is 24).

## Compatible representation:

AI\_DES\_EDE3\_CBCPadBER.

## Output considerations:

During encryption, this AI pads the output (which DES requires to be a multiple of 8 bytes long). Thus, the total number of output bytes from encryption can be as many as 8 bytes more than the total output.

## AI\_DESX\_CBC\_BSAFE1

### Purpose:

Deprecated. This AI is included only for backward compatibility.

### Type of information this allows you to use:

the encryption type parameter (pad, pad with checksum, or raw) for the DESX encryption algorithm as defined by BSAFE 1.x.

### Format of *info* supplied to `B_SetAlgorithmInfo`:

pointer to a `B_BSAFE1_ENCRYPTI ON_PARAMS` structure:

```
typedef struct {
    int encrypti onType;           /* encryption type */
} B_BSAFE1_ENCRYPTI ON_PARAMS;
```

*encrypti onType* should be set to `B_BSAFE1_PAD` for pad mode, `B_BSAFE1_PAD_CHECKSUM` for pad with checksum mode, or `B_BSAFE1_RAW` for raw mode.

### Format of *info* returned by `B_GetAlgorithmInfo`:

pointer to a `B_BSAFE1_ENCRYPTI ON_PARAMS` structure (see above).

### Crypto-C procedures to use with algorithm object:

`B_EncryptI nit`, `B_EncryptUpdate`, `B_EncryptFi nal`, `B_DecryptI nit`, `B_DecryptUpdate`, and `B_DecryptFi nal`. You may pass `(B_ALGORI THM_OBJ) NULL_PTR` for all *randomAl gori thm* arguments.

### Algorithm methods to include in application's algorithm chooser:

`AM_DESX_CBC_ENCRYPT` for encryption and `AM_DESX_CBC_DECRYPT` for decryption.

### Key info types for *keyObject* in `B_EncryptInit` or `B_DecryptInit`:

`KI_DES24Strong`, `KI_24Byte`, `KI_I tem` (if the length of the `I TEM` is 24), `KI_DESX` or `KI_DESX_BSAFE1`.

**Input constraints:**

During encryption, this algorithm does not pad the output. Thus, you must provide input that is a multiple of 8 bytes.

**Output considerations:**

In pad mode, the total number of output bytes from encryption can be as many as eight more than the total input. In pad with checksum mode, the total number of output bytes from encryption can be as many as 16 more than the total input.

## AI\_DESX\_CBC\_IV8

### Purpose:

This AI allows you to perform DESX encryption or decryption in CBC mode with an 8-byte initialization vector on data that is a multiple of 8 bytes long. This algorithm takes 24 bytes of keying material. The first 8 bytes of the key form a standard 56-bit DES key, the second 8 bytes become the input whitening, and the last 8 bytes become the output whitening. The DESX algorithm has 64-bit input and output blocks like DES and it is used in all the same modes. Internally, the plaintext is exclusive-or'ed with the input whitening before running it through a DES encryption; and the output of DES is exclusive-or'ed with the output whitening to produce the output block of DESX. Decryption reverses those steps. See AI\_DESX\_CBCPadI V8 for the same algorithm type with padding.

### Type of information this allows you to use:

an 8-byte initialization vector for the DESX-CBC encryption algorithm, as defined by RSA Data Security, Inc.

### Format of *info* supplied to B\_SetAlgorithmInfo:

pointer to an unsigned char array that holds the 8 bytes of the initialization vector.

### Format of *info* returned by B\_GetAlgorithmInfo:

pointer to an unsigned char array that holds the 8 bytes of the initialization vector.

### Crypto-C procedures to use with algorithm object:

B\_EncryptInit, B\_EncryptUpdate, B\_EncryptFinal, B\_DecryptInit, B\_DecryptUpdate, and B\_DecryptFinal. You may pass (B\_ALGORITHM\_OBJ)NULL\_PTR for all *randomAlgorithm* arguments.

### Algorithm methods to include in application's algorithm chooser:

AM\_DESX\_CBC\_ENCRYPT for encryption and AM\_DESX\_CBC\_DECRYPT for decryption.

### Key info types for *keyObject* in B\_EncryptInit or B\_DecryptInit:

KI\_DES24Strong, KI\_24Byte, KI\_Item (if the length of the ITEM is 24), KI\_DESX, or

KI\_DESX\_BSAFE1.

### **Input constraints:**

During encryption, this algorithm does not pad the output. Thus, you must provide input that is a multiple of 8 bytes.

## AI\_DESX\_CBCPadBER

### Purpose:

This AI is similar to AI\_DESX\_CBCPadV8 except that it uses the ASN.1 BER format. This AI allows you to parse and create ASN.1 algorithm identifiers, such as used in PKCS #7, and other protocols. You call B\_SetAlgorithmInfo to initialize an algorithm object from the encoded algorithm identifier that includes the initialization vector. Alternatively, you call B\_GetAlgorithmInfo with this AI to create an encoded algorithm identifier from an algorithm object that was created using AI\_DESX\_CBCPadV8 or AI\_DESX\_CBCPadBER. The OID for this algorithm—excluding the tag and length bytes—in decimal, is "42, 134, 72, 134, 247, 13, 3, 6". Also see AI\_DESX\_CBCPadV8.

### Type of information this allows you to use:

the encoded algorithm identifier that specifies the DESX-CBC encryption algorithm, as defined by RSA Data Security, Inc., with padding scheme defined in PKCS #5.

### Format of *info* supplied to B\_SetAlgorithmInfo:

pointer to an ITEM structure that gives the address and length of the BER-encoded algorithm identifier. The encoding is converted to DER before it is copied to the algorithm object. B\_SetAlgorithmInfo returns BE\_WRONG\_ALGORITHM\_INFO if the algorithm identifier specifies an algorithm other than DESX-CBC With Padding.

### Format of *info* returned by B\_GetAlgorithmInfo:

pointer to an ITEM structure that gives the address and length of the DER-encoded algorithm identifier.

### Crypto-C procedures to use with algorithm object:

B\_EncryptInit, B\_EncryptUpdate, B\_EncryptFinal, B\_DecryptInit, B\_DecryptUpdate, and B\_DecryptFinal. You may pass (B\_ALGORITHM\_OBJ)NULL\_PTR for all *randomAlgorithm* arguments.

### Algorithm methods to include in application's algorithm chooser:

AM\_DESX\_CBC\_ENCRYPT for encryption and AM\_DESX\_CBC\_DECRYPT for decryption.

**Key info types for *keyObject* in B\_EncryptInit or B\_DecryptInit:**

KI\_DES24Strong, KI\_24Byte, KI\_Item (if the length of the ITEM is 24), KI\_DESX, or KI\_DESX\_BSAFE1.

**Compatible representation:**

AI\_DESX\_CBCPadV8.

**Output considerations:**

During encryption, this AI pads the output (which DES requires to be a multiple of 8 bytes long). Thus, the total number of output bytes from encryption can be as many as 8 bytes more than the total output.

## AI\_DESX\_CBCPadIV8

### Purpose:

This AI allows you to perform DESX encryption or decryption in CBC mode. It is initialized with an 8-byte IV and operates on data that is any byte length. The padding mode is PKCS #5, which makes the ciphertext 1 to 8 bytes longer than the plaintext. See AI\_DESX\_CBC\_IV8 for the same algorithm type with no padding. See AI\_DESX\_CBCPadBER for the same algorithm type with BER encoding.

### Type of information this allows you to use:

an 8-byte initialization vector for the DESX-CBC encryption algorithm, as defined by RSA Data Security, Inc., with padding scheme defined in PKCS #5.

### Format of *info* supplied to B\_SetAlgorithmInfo:

pointer to an unsigned char array that holds the 8 bytes of the initialization vector.

### Format of *info* returned by B\_GetAlgorithmInfo:

pointer to an unsigned char array that holds the 8 bytes of the initialization vector.

### Crypto-C procedures to use with algorithm object:

B\_EncryptInit, B\_EncryptUpdate, B\_EncryptFinal, B\_DecryptInit, B\_DecryptUpdate, and B\_DecryptFinal. You may pass (B\_ALGORITHM\_OBJ)NULL\_PTR for all *randomAlgorithm* arguments.

### Algorithm methods to include in application's algorithm chooser:

AM\_DESX\_CBC\_ENCRYPT for encryption and AM\_DESX\_CBC\_DECRYPT for decryption.

### Key info types for *keyObject* in B\_EncryptInit or B\_DecryptInit:

KI\_DES24Strong, KI\_24Byte, KI\_Item (if the length of the ITEM is 24), KI\_DESX, or KI\_DESX\_BSAFE1.

### Compatible representation:

AI\_DESX\_CBCPadBER.

## Output considerations:

During encryption, this AI pads the output (which DES requires to be a multiple of 8 bytes long). Thus, the total number of output bytes from encryption can be as many as 8 bytes more than the total output.

# AI\_DHKeyAgree

## Purpose:

This AI allows you to perform Diffie-Hellman key agreement. You may have generated system parameters (for example, through AI\_DHParamGen), or you may have retrieved them from another source. These system parameters are passed to B\_SetAlgorithmInfo. The function B\_KeyAgreePhase1 creates the public value that is sent to the other party, and B\_KeyAgreePhase2 processes the value from the other party to produce the shared secret value. See AI\_DHKeyAgreeBER for the same algorithm type with BER encoding.

## Type of information this allows you to use:

Diffie-Hellman system parameters, where the prime and base integers, and the exponent size, are specified for performing Diffie-Hellman key agreement as defined in PKCS #3.

## Format of *info* supplied to B\_SetAlgorithmInfo:

pointer to an A\_DH\_KEY\_AGREE\_PARAMS structure:

```
typedef struct {
    ITEM          prime;                /* prime modulus */
    ITEM          base;                 /* base generator */
    unsigned int exponentBits;        /* size of random exponent in bits */
} A_DH_KEY_AGREE_PARAMS;
```

Each ITEM supplies an integer in canonical format, where the ITEM's *data* points to an unsigned byte array -- most significant byte first -- and the ITEM's *len* gives its length. All leading zeros are stripped from each integer before it is copied to the algorithm object.

## Format of *info* returned by B\_GetAlgorithmInfo:

pointer to an A\_DH\_KEY\_AGREE\_PARAMS structure (see above). All leading zeros have been stripped from each integer in the structure.

## Crypto-C procedures to use with algorithm object:

B\_KeyAgreeInit, B\_KeyAgreePhase1, and B\_KeyAgreePhase2. You must pass an

initialized random algorithm to B\_KeyAgreePhase1.

## Algorithm methods to include in application's algorithm chooser:

AM\_DH\_KEY\_AGREE.

## Compatible representation:

AI\_DHKeyAgreeBER.

## Output considerations:

The size of the output of B\_KeyAgreePhase1 (the public value) will be the same size as the *prime*. The size of the output of B\_KeyAgreePhase2 (the agreed-upon secret) will also be the same size as the *prime*.

## AI\_DHKeyAgreeBER

### Purpose:

This AI is similar to AI\_DHKeyAgree except that it uses the ASN.1 BER format. This AI allows you to parse and create ASN.1 algorithm identifiers such as used in PKCS #7 and other protocols. You call B\_SetAlgorithmInfo to initialize an algorithm object from the encoded algorithm identifier that includes the prime modulus, base, and private value length. Alternatively, you call B\_GetAlgorithmInfo with this AI to create an encoded algorithm identifier from an algorithm object that was created using AI\_DHKeyAgree or AI\_DHKeyAgreeBER. The OID for this algorithm, excluding the tag and length bytes, in decimal, is "42, 134, 72, 134, 247, 13, 1, 3, 1". Also see AI\_DHKeyAgree.

### Type of information this allows you to use:

the encoded algorithm identifier that specifies Diffie-Hellman key agreement as defined in PKCS #3.

### Format of *info* supplied to B\_SetAlgorithmInfo:

pointer to an ITEM structure that gives the address and length of the BER-encoded algorithm identifier. The encoding is converted to DER before it is copied to the algorithm object. B\_SetAlgorithmInfo returns BE\_WRONG\_ALGORITHM\_INFO if the algorithm identifier specifies an algorithm other than Diffie-Hellman.

### Format of *info* returned by B\_GetAlgorithmInfo:

pointer to an ITEM structure that gives the address and length of the DER-encoded algorithm identifier.

### Crypto-C procedures to use with algorithm object:

B\_KeyAgreeInit, B\_KeyAgreePhase1, and B\_KeyAgreePhase2. You must pass an initialized random algorithm to B\_KeyAgreePhase1.

### Algorithm methods to include in application's algorithm chooser:

AM\_DH\_KEY\_AGREE.

## Compatible representation:

AI\_DHKeyAgree.

## Output considerations:

The size of the output of B\_KeyAgreePhase1 (the public value) will be the same size as the *prime*. The size of the output of B\_KeyAgreePhase2 (the agreed-upon secret) will also be the same size as the *prime*.

## AI\_DHParamGen

### Purpose:

This AI allows you to generate Diffie-Hellman system parameters, which are the prime modulus, base, and private value length.

### Type of information this allows you to use:

the parameters for generating Diffie-Hellman system parameters as defined in PKCS #3, where the size of the prime modulus and random exponent are specified. The optimized generating algorithm is proprietary, as defined by RSA Data Security, Inc.

### Format of *info* supplied to B\_SetAlgorithmInfo:

pointer to an A\_DH\_PARAM\_GEN\_PARAMS structure:

```
typedef struct {
    unsigned int primeBits;           /* size of prime modulus in bits */
    unsigned int exponentBits;       /* size of random exponent in bits */
} A_DH_PARAM_GEN_PARAMS;
```

The *exponentBits* must be less than *primeBits*.

### Format of info returned by B\_GetAlgorithmInfo:

pointer to an A\_DH\_PARAM\_GEN\_PARAMS structure (see above).

### Crypto-C procedures to use with algorithm object:

B\_GenerateInt and B\_GenerateParameters. B\_GenerateParameters sets the *resultAlgorithmObject* with the AI\_DHKeyAgree information. You must pass an initialized random algorithm to B\_GenerateParameters.

### Algorithm methods to include in application's algorithm chooser:

AM\_DH\_PARAM\_GEN.

## AI\_DSA

### Purpose:

This AI allows you to create or verify raw DSA signatures when the 20-byte input is already known. It does not compute a message digest before applying the signature operation. See AI\_DSAAwithSHA1 for the DSA algorithm type that involves the SHA1 digest operation.

### Type of information this allows you to use:

the DSA signature algorithm for performing raw DSA signing and verifying as defined in FIPS PUB 186.

### Format of *info* supplied to B\_SetAlgorithmInfo:

NULL\_PTR.

### Format of *info* returned by B\_GetAlgorithmInfo:

NULL\_PTR.

### Crypto-C procedures to use with algorithm object:

B\_SignInit, B\_SignUpdate, B\_SignFinal, B\_VerifyInit, B\_VerifyUpdate, and B\_VerifyFinal. You must pass a random algorithm in B\_SignFinal, but may pass (B\_ALGORITHM\_OBJ) NULL\_PTR for all other *randomAlgorithm* arguments.

### Algorithm methods to include in application's algorithm chooser:

AM\_DSA\_SIGN for signature creation and AM\_DSA\_VERIFY for signature verification.

### Key info types for *keyObject* in B\_SignInit:

KI\_DSAPrivate, KI\_DSAPrivateBER, or KI\_DSAPrivateX957BER.

### Key info types for *keyObject* in B\_VerifyInit:

KI\_DSAPublic, KI\_DSAPublicBER, or KI\_DSAPublicX957BER.

## Input constraints:

The DSA algorithm requires that the input data (the data to sign) be exactly 20 bytes long. Normally, this 20-byte input is the result of SHA1 output.

## Output considerations:

The *signature* result of `B_SignFinal` will be 40 bytes long; these bytes appear in the order  $(r, s)$ .

## Token-based algorithm methods:



AI\_DSA may be used to access the hardware-related algorithm methods `AM_TOKEN_DSA_SIGN` and `AM_TOKEN_DSA_VERIFY` for use with BHAPI.

## Token-based key info types:

When used with one of the hardware algorithm methods listed above, AI\_DSA should be used with `KI-Token` or `KI_KeypairToken`.

## AI\_DSASKeyGen

### Purpose:

This AI allows you to generate a DSA key pair. First, you pass the system parameters to `B_SetAlgorithmInfo`. Then you generate the keys by calling `B_GenerateInit` and `B_GenerateKeyPair`. Alternatively, you may use the `AI_DSASParamGen` algorithm type to generate the system parameters needed in DSA key generation. Also see `AI_DSASParamGen`.

### Type of information this allows you to use:

the parameters for generating a compatible DSA key pair as defined in FIPS PUB 186.

### Format of *info* supplied to `B_SetAlgorithmInfo`:

pointer to an `A_DSA_PARAMS` structure:

```
typedef struct {
    ITEM prime;                /* the prime p */
    ITEM subPrime;            /* the subprime q */
    ITEM base;                /* the base g */
} A_DSA_PARAMS;
```

An `ITEM` supplies an integer in canonical format, where the `ITEM`'s *data* points to an unsigned byte array -- most significant byte first -- and the `ITEM`'s *len* gives its length. All leading zeros are stripped from the integer before it is copied to the algorithm object.

### Format of *info* returned by `B_GetAlgorithmInfo`:

pointer to an `A_DSA_PARAMS` structure (see above).

### Crypto-C procedures to use with algorithm object:

`B_GenerateInit` and `B_GenerateKeyPair`. `B_GenerateKeyPair` sets the *publicKey* key object with the `KI_DSAPublic` information and the *privateKey* key object with the `KI_DSAPrivate` information. You must pass an initialized random algorithm to `B_GenerateKeyPair`.

**Algorithm methods to include in application's algorithm chooser:**

AM\_DSA\_KEY\_GEN.

## AI\_DSAParamGen

### Purpose:

This AI allows you to generate DSA system parameters. The sizes of the parameters are passed to `B_SetAlgorithmInfo` and the parameters are made by calling `B_GenerateInit` and `B_GenerateParameters`. You use DSA parameters generated by this AI to generate a DSA key pair. Also see `AI_DSASKeyGen`.

### Type of information this allows you to use:

the number of prime bits for generating a prime, a subprime, and a base ( $p$ ,  $q$ , and  $g$ ) compatible with FIPS PUB 186.

### Format of *info* supplied to `B_SetAlgorithmInfo`:

pointer to a `B_DSA_PARAM_GEN_PARAMS` structure:

```
typedef struct {
    unsigned int primeBits;           /* size of prime in bits */
} B_DSA_PARAM_GEN_PARAMS;
```

### Format of *info* returned by `B_GetAlgorithmInfo`:

pointer to a `B_DSA_PARAM_GEN_PARAMS` structure (see above).

### Crypto-C procedures to use with algorithm object:

`B_GenerateInit` and `B_GenerateParameters`. `B_GenerateParameters` sets the *resultAlgorithmObject* algorithm object with the `AI_DSASKeyGen` information. You must pass an initialized random algorithm to `B_GenerateParameters`.

### Algorithm methods to include in application's algorithm chooser:

`AM_DSA_PARAM_GEN`.

### Notes:

The size of the subprime is always 160 bits.

---

## AI\_DSAShA1

### Purpose:

This AI allows you to create or verify SHA1 DSA signatures. It is passed the plaintext and computes the SHA1 digest as well as the DSA signature of that digest. See AI\_DSA for the DSA algorithm type without the SHA1 digest operation. See AI\_DSAShA1\_BER for the same algorithm type with BER encoding.

### Type of information this allows you to use:

the DSA With SHA1 signature algorithm that uses the SHA1 digest algorithm and DSA to create and verify DSA digital signatures as defined in X9.57 Draft Section 5.3.1 and FIPS PUB 186.

### Format of *info* supplied to B\_SetAlgorithmInfo:

NULL\_PTR.

### Format of *info* returned by B\_GetAlgorithmInfo:

NULL\_PTR.

### Crypto-C procedures to use with algorithm object:

B\_SignInit, B\_SignUpdate, B\_SignFinal, B\_VerifyInit, B\_VerifyUpdate, and B\_VerifyFinal. You must pass a random algorithm in B\_SignFinal, but may pass (B\_ALGORITHM\_OBJ) NULL\_PTR for all other *randomAlgorithm* arguments.

### Algorithm methods to include in application's algorithm chooser:

AM\_SHA and AM\_DSASIGN for signature creation, and AM\_DSASVERIFY for signature verification.

### Key info types for *keyObject* in B\_SignInit:

KI\_DSAPrivate, KI\_DSAPrivateBER, or KI\_DSAPrivateX957BER.

### Key info types for *keyObject* in B\_VerifyInit:

KI\_DSAPublic, KI\_DSAPublicBER, or KI\_DSAPublicX957BER.

## Compatible representation:

AI\_DSAWithSHA1\_BER.

## Output considerations:

The *signature* result of `B_SignFinal` is a BER-encoded value of type SEQUENCE (INTEGER, INTEGER), where the first field is the value  $r$  and the second field is the value  $s$  as defined in section 5.3.1 of X9.57 Draft. The size of *signature* may be as many as 48 bytes.

## AI\_DSAShSHA1\_BER

### Purpose:

This AI is similar to AI\_DSAShSHA1 except that it uses the ASN.1 BER format. This AI allows you to parse and create ASN.1 algorithm identifiers such as used in PKCS #7 and other protocols. You call `B_SetAlgorithmInfo` to initialize an algorithm object from the encoded algorithm identifier. You call `B_GetAlgorithmInfo` with this AI to create an encoded algorithm identifier from an algorithm object that was created using AI\_DSAShSHA1 or AI\_DSAShSHA1\_BER. The OID for this algorithm, excluding the tag and length bytes, in decimal, is "43, 14, 3, 2, 27". Also see AI\_DSAShSHA1.

### Type of information this allows you to use:

the encoding of an algorithm identifier that specifies the DSA With SHA1 signature algorithm that uses the SHA1 digest algorithm and DSA to create and verify DSA digital signatures as defined in X9.57 Draft Section 5.3.1 and FIPS PUB 186.

### Format of *info* supplied to `B_SetAlgorithmInfo`:

pointer to an `ITEM` structure that gives the address and length of the BER-encoded algorithm identifier. The encoding is converted to DER before it is copied to the algorithm object. `B_SetAlgorithmInfo` returns `BE_WRONG_ALGORITHM_INFO` if the algorithm identifier specifies an algorithm other than DSA With SHA1.

### Format of *info* returned by `B_GetAlgorithmInfo`:

pointer to an `ITEM` structure that gives the address and length of the DER-encoded algorithm identifier.

### Crypto-C procedures to use with algorithm object:

`B_SignInit`, `B_SignUpdate`, `B_SignFinal`, `B_VerifyInit`, `B_VerifyUpdate`, and `B_VerifyFinal`. You must pass a random algorithm in `B_SignFinal`, but may pass `(B_ALGORITHM_OBJ)NULL_PTR` for all other *randomAlgorithm* arguments.

### Algorithm methods to include in application's algorithm chooser:

`AM_SHA1` and `AM_DSA_SIGN` for signature creation, and `AM_DSA_VERIFY` for signature verification.

### Key info types for *keyObject* in B\_SignInit:

KI\_DSAPri vate, KI\_DSAPri vateBER, or KI\_DSAPri vateX957BER.

### Key info types for *keyObject* in B\_VerifyInit:

KI\_DSAPubl i c, KI\_DSAPubl i cBER, or KI\_DSAPubl i cX957BER.

### Compatible representation:

AI\_DSAWi thSHA1.

### Output considerations:

The *signature* result of B\_Si gnFi nal is a BER-encoded value of type SEQUENCE (INTEGER, INTEGER) where the first field is the value *r* and the second field is the value *s* as defined in section 5.3.1 of X9.57 Draft. The size of *signature* may be as many as 48 bytes.

## AI\_ECAcceleratorTable

### Purpose:

This AI allows you to use the acceleration table for various elliptic curve (EC) operations that include encryption, signature creation and verification, key pair generation, and key agreement operations.

### Type of information this allows you to use:

the acceleration table produced by the operation of `AI_ECBuildAcceleratorTable` on EC parameters or the table produced by the operation of `AI_ECBuildPublicKeyAcceleratorTable` on EC parameters.

### Format of *info* supplied to `B_SetAlgorithmInfo`:

pointer to an `ITEM` holding the accelerator table.

### Format of *info* returned by `B_GetAlgorithmInfo`:

pointer to an `ITEM` holding the accelerator table.

### Crypto-C procedures to use with algorithm object:

you use the table generated by `AI_ECBuildAcceleratorTable` with `B_SetAlgorithmInfo` to accelerate EC encryption in `AI_EC_ES`, signature creation and verification in `AI_EC_DSA` and `AI_EC_DSASign`, key pair generation in `AI_ECKeyGen`, and phase 1 of key agreement operations in `AI_EC_DHKeyAgree`. Use the table generated by `AI_ECBuildPublicKeyAcceleratorTable` with `B_SetAlgorithmInfo` to accelerate verification in `AI_EC_DSA` and `AI_EC_DSASign`.

### Algorithm methods to include in application's algorithm chooser:

None.

## AI\_ECBuildAcceleratorTable

### Purpose:

This AI allows you to build an acceleration table for the retrieval of a base point in various elliptic curve (EC) operations. To build a table that includes public key values as well as base point values, see AI\_ECBuildPubKeyAcceleratorTable.

### Type of information this allows you to use:

elliptic curve parameters as defined in X9.62 Draft to generate auxiliary data for the acceleration of EC operations with base point. Elliptic curve parameters can be generated through the execution of AI\_ECParamGen.

### Format of *info* supplied to B\_SetAlgorithmInfo:

pointer to a B\_EC\_PARAMS structure:

```
typedef struct {
    B_INFO_TYPE parameterInfoType;          /* used to interpret EC parameters */
    POINTER     parameterInfoValue        /* describes elliptic curve */
} B_EC_PARAMS;
```

where *parameterInfoType* must be AI\_ECParameters and *parameterInfoValue* must be an A\_EC\_PARAMS structure:

```
typedef struct {
    unsigned int version;                    /* implementation version */
    unsigned int fieldType;                 /* indicates type of base field */
    ITEM        fieldInfo;                 /* It is the prime number */
                                           /* if fieldType = FT_FP; */
                                           /* the basis polynomial if fieldType = FT_F2_POLYNOMIAL; */
                                           /* and the degree of the field if fieldType = FT_F2_ONB */
    ITEM        coeffA;                    /* elliptic curve coefficient */
    ITEM        coeffB;                    /* elliptic curve coefficient */
    ITEM        base;                      /* elliptic curve group generator */
    ITEM        order;                     /* order of subgroup's generating element */
    ITEM        cofactor;                 /* the cofactor of the subgroup */
    unsigned int compressIndicator;       /* controls field element representation */
    unsigned int fieldElementBits;       /* field element size in bits */
} A_EC_PARAMS;
```

## Format of *info* returned by B\_GetAlgorithmInfo:

B\_GetAlgorithmInfo is not supported with this AI. If called, it will return an error.

## Crypto-C procedures to use with algorithm object:

B\_BuildTableInit and B\_BuildTableFinal.

## Algorithm methods to include in application's algorithm chooser:

AM\_ECFP\_BLD\_ACCEL\_TABLE for odd prime fields and AM\_ECF2POLY\_BLD\_ACCEL\_TABLE for even characteristic.

## Output Considerations:

The size of the accelerator table may be found through a call to B\_BuildTableGetBufSize after a call to B\_BuildTableInit.

## AI\_ECBuildPubKeyAccelTable

### Purpose:

This AI allows you to build an acceleration table for a public key and the base point to be used in various elliptic curve (EC) operations. The acceleration values come from a table that includes values built for the base point, which are the same as those from AI\_ECBuildAccelTable, and additional values built for the public key. This AI performs at greater speeds than AI\_ECBuildAccelTable for both ECDSA verify and ECDH Phase 2 operations.

### Type of information this allows you to use:

elliptic curve parameters as defined in X9.62 Draft to generate auxiliary data for the acceleration of elliptic curve operations with base point and public key. Elliptic curve parameters can be generated through the execution of AI\_ECParamGen.

### Format of *info* supplied to B\_SetAlgorithmInfo:

pointer to a B\_EC\_PARAMS structure:

```
typedef struct {
    B_INFO_TYPE parameterInfoType;          /* used to interpret EC parameters */
    POINTER     parameterInfoValue         /* describes elliptic curve */
} B_EC_PARAMS;
```

where *parameterInfoType* must be AI\_ECPubKey and *parameterInfoValue* must be an A\_EC\_PUBLIC\_KEY structure:

```
typedef struct {
    ITEM        publicKey;                  /* public component */
    A_EC_PARAMS curveParams;               /* the underlying elliptic curve parameters */
} A_EC_PUBLIC_KEY;
```

### Format of *info* returned by B\_GetAlgorithmInfo:

B\_GetAlgorithmInfo is not supported with this AI. If called, it will return an error.

## Crypto-C procedures to use with algorithm object:

B\_BuildTableInit and B\_BuildTableFinal.

## Algorithm methods to include in application's algorithm chooser:

AM\_ECFP\_BLD\_PUB\_KEY\_ACCEL\_TABLE for odd prime fields and  
AM\_ECF2POLY\_BLD\_PUB\_KEY\_ACCEL\_TABLE for even characteristic.

## Output Considerations:

The size of the accelerator table may be found through a call to  
B\_BuildTableGetBufSize after a call to B\_BuildTableInit.

# AI\_EC\_DHKeyAgree

## Purpose:

This AI allows you to perform elliptic curve Diffie-Hellman key agreement for given EC parameters. You may have generated system parameters (for example, through AI\_ECPParamGen), or you may have retrieved them from another source. These system parameters are passed to B\_SetAlgorithmInfo. The function B\_KeyAgreePhase1 creates the public value that is sent to the other party, and B\_KeyAgreePhase2 processes the value from the other party to produce the shared secret value.

## Type of information this allows you to use:

elliptic curve system parameters used in the elliptic curve, Diffie-Hellman key agreement operation, as defined in X9.63 Draft.

## Format of *info* supplied to B\_SetAlgorithmInfo:

pointer to a B\_EC\_PARAMS structure:

```
typedef struct {
    B_INFO_TYPE *parameterInfoType;      /* used to interpret EC parameters */
    POINTER      parameterInfoValue;     /* describes elliptic curve */
} B_EC_PARAMS;
```

where *parameterInfoType* must be AI\_ECParameters and *parameterInfoValue* must be an A\_EC\_PARAMS structure:

```
typedef struct {
    unsigned int  version;                /* implementation version */
    unsigned int  fieldType;              /* indicates type of base field */
    ITEM          fieldInfo;              /* The prime number if fieldType = FT_FP;
                                           /* the basis polynomial if fieldType = FT_F2_POLYNOMIAL;
                                           /* and the degree of the field if fieldType = FT_F2_ONB */
    ITEM          coeffA;                  /* elliptic curve coefficient */
    ITEM          coeffB;                  /* elliptic curve coefficient */
    ITEM          base;                    /* elliptic curve group generator */
    ITEM          order;                   /* order of subgroup's generating element */
    ITEM          cofactor;               /* the cofactor of the subgroup */
    unsigned int  compressIndicator;      /* controls field element representation */
    unsigned int  fieldElementBits;      /* field element size in bits */
} A_EC_PARAMS;
```

## Format of *info* returned by B\_GetAlgorithmInfo:

B\_GetAlgorithmInfo is not supported with this AI. If called, it will return an error.

## Crypto-C procedures to use with algorithm object:

B\_KeyAgreeInit, B\_KeyAgreePhase1, and B\_KeyAgreePhase2. You must pass an initialized random algorithm to B\_KeyAgreePhase1.

## Algorithm methods to include in application's algorithm chooser:

AM\_ECFP\_DH\_KEY\_AGREE for odd prime fields and AM\_ECF2POLY\_DH\_KEY\_AGREE for even characteristic.

## Output considerations:

The size of Phase 1 output is  $1 + 2 \cdot (\text{size of field element})$  bytes; the size of Phase 2 output is the  $(\text{size of field element})$  bytes

## AI\_EC\_DSA

### Purpose:

This AI allows you to perform raw ECDSA signature creation or verification operations. It does not compute a message digest before applying the signature operation. To compute a SHA1 message digest and create a signature of that digest, see AI\_EC\_DSAwithDigest.

### Type of information this allows you to use:

the ECDSA signature algorithm used in raw ECDSA signature generation and verification, as defined in X9.62 Draft. Alternatively, to use an acceleration table in the generation or verification of a signature, use AI\_ECBuildAcceleratorTable or AI\_ECBuildPublicKeyAcceleratorTable. The public key-specific acceleration table accelerates verification only; for this operation, it provides greater acceleration than the AI\_ECBuildAcceleratorTable at the cost of greater memory usage.

### Format of *info* supplied to B\_SetAlgorithmInfo:

NULL\_PTR.

### Format of *info* returned by B\_GetAlgorithmInfo:

NULL\_PTR.

### Crypto-C procedures to use with algorithm object:

B\_SignInit, B\_SignUpdate, B\_SignFinal, B\_VerifyInit, B\_VerifyUpdate, and B\_VerifyFinal. You must pass a random algorithm in B\_SignFinal, but may pass (B\_ALGORITHM\_OBJ) NULL\_PTR for all other *randomAlgorithm* arguments.

### Algorithm methods to include in application's algorithm chooser:

For signature creation, AM\_ECFP\_DSA\_SIGN for odd prime fields and AM\_ECF2POLY\_DSA\_SIGN for even characteristic. For signature verification, AM\_ECFP\_DSA\_VERIFY for odd prime fields and AM\_ECF2POLY\_DSA\_VERIFY for even characteristic.

## Key info types for keyObject in B\_SignInit:

KI\_ECPrivate.

## Key info types for keyObject in B\_VerifyInit:

KI\_ECPublic.

## Input constraints:

In practice, the input to the ECDSA algorithm — that is, the data to sign — is generally the result of a digest operation. In Crypto-C's implementation, however, the only restrictions on the input are that it must be at least 16 bytes and no more than 32 bytes long.

## Output considerations:

The signature result of `B_SignFinal` is a value of type SEQUENCE (INTEGER, INTEGER) where the first field is the value  $r$  and the second field is the value  $s$ , as defined in section 5.3.1 of X9.57 Draft. The size of *signature* is  $2 \times (\text{length of order})$  bytes. For instance, if the order is 160 bits (20 bytes), the *signature* will be 40 bytes long.

## AI\_EC\_DSASWithDigest

### Purpose:

This AI allows you to create or verify SHA1 ECDSA signatures. It is passed the plaintext and computes the SHA1 digest as well as the ECDSA signature of that digest. See AI\_EC\_DSA for the ECDSA algorithm type without the SHA1 digest.

### Type of information this allows you to use:

the specified digest algorithm combined with the ECDSA signature algorithm for performing ECDSA signing and verifying as defined in X9.62 Draft. The only digest method supported in this API is SHA1.

### Format of *info* supplied to B\_SetAlgorithmInfo:

pointer to a B\_DIGEST\_SPECIFIER structure:

```
typedef struct {
    B_INFO_TYPE digestInfoType;
    POINTER digestInfoParams;
} B_DIGEST_SPECIFIER;
```

Crypto-C 4.2 supports only AI\_SHA1 as a *digestInfoType*, with NULL\_PTR as the *digestInfoParams*.

### Format of *info* returned by B\_GetAlgorithmInfo:

pointer to a B\_DIGEST\_SPECIFIER structure.

### Crypto-C procedures to use with algorithm object:

B\_SignInit, B\_SignUpdate, B\_SignFinal, B\_VerifyInit, B\_VerifyUpdate, and B\_VerifyFinal. You must pass an initialized random algorithm in B\_SignFinal, but may pass (B\_ALGORITHM\_OBJ)NULL\_PTR for all other *randomAlgorithm* arguments.

### Algorithm methods to include in application's algorithm chooser:

For signing, AM\_ECFDSA\_SIGN for odd prime fields and AM\_ECF2POLY\_DSA\_SIGN for an even characteristic. For verifying, AM\_ECFDSA\_VERIFY for odd prime fields and AM\_ECF2POLY\_DSA\_VERIFY for even characteristic. Also required is the appropriate AM

for the digest specified, for instance, AM\_SHA when the *digestInfoType* is AI\_SHA1.

### Key info types for keyObject in B\_SignInit:

KI\_ECPrivate.

### Key info types for keyObject in B\_VerifyInit:

KI\_ECPublic.

### Output considerations:

The *signature* result of B\_SignFinal is a BER-encoded value of type SEQUENCE (INTEGER, INTEGER) where the first field is the value  $r$  and the second field is the value  $s$ , as defined in section 5.3.1 of X9.57 Draft. The size of *signature* is  $6 + (2 \cdot (\text{length of order}))$  bytes. For instance, if the order is 160 bits (20 bytes), the *signature* will be 46 bytes long.

---

## AI\_EC\_ES

### Purpose:

This AI allows you to perform public-key encryption or private-key decryption using the Elliptic-Curve Authenticated Encryption System, where ciphertext includes the SHA1 digest as well as encrypted plaintext.

### Type of information this allows you to use:

the elliptic curve authenticated encryption scheme as defined in X9.63 Draft, as of 10/97.

### Format of *info* supplied to `B_SetAlgorithmInfo`:

NULL\_PTR.

### Format of *info* returned by `B_GetAlgorithmInfo`:

NULL\_PTR.

### Crypto-C procedures to use with algorithm object:

`B_EncryptInit`, `B_EncryptUpdate`, `B_EncryptFinal`, `B_DecryptInit`, `B_DecryptUpdate`, and `B_DecryptFinal`. You must pass an initialized random algorithm in `B_EncryptFinal`, but may pass `(B_ALGORITHM_OBJ) NULL_PTR` for all other *randomAlgorithm* arguments.

### Algorithm methods to include in application's algorithm chooser:

`AM_ECFP_ENCRYPT` for encryption and `AM_ECFP_DECRYPT` for decryption with odd prime fields, `AM_ECF2POLY_ENCRYPT` for encryption and `AM_ECF2POLY_DECRYPT` for decryption with even characteristic.

### Output Considerations:

The encrypted data can be as much as  $((21 + 2 \cdot (\text{the size of a field element in bytes}) + (\text{length of input in bytes}))$  bytes long.

## AI\_ECKeyGen

### Purpose:

This AI allows you to generate an elliptic curve key pair for given EC parameters.

### Type of information this allows you to use:

the parameters for generating a compatible elliptic curve key pair. The precomputed table values from AI\_ECAcceleratorTable can optionally be used to accelerate this operation.

### Format of *info* supplied to B\_SetAlgorithmInfo:

pointer to a B\_EC\_PARAMS structure:

```
typedef struct {
    B_INFO_TYPE parameterInfoType;          /* used to interpret EC parameters */
    POINTER     parameterInfoValue;        /* describes elliptic curve */
} B_EC_PARAMS;
```

where *parameterInfoType* must be AI\_ECParameters and *parameterInfoValue* must be a pointer to an A\_EC\_PARAMS structure:

```
typedef struct {
    unsigned int version;                    /* implementation version */
    unsigned int fieldType;                  /* indicates type of base field */
    ITEM        fieldInfo;                  /* The prime number if fieldType = FT_FP; */
                                           /* the basis polynomial if fieldType = FT_F2_POLYNOMIAL; */
                                           /* and the degree of the field if fieldType = FT_F2_ONB */
    ITEM        coeffA;                      /* elliptic curve coefficient */
    ITEM        coeffB;                      /* elliptic curve coefficient */
    ITEM        base;                        /* elliptic curve group generator */
    ITEM        order;                      /* order of subgroup's generating element */
    ITEM        cofactor;                   /* the cofactor of the subgroup */
    unsigned int compressIndicator;        /* controls field element representation */
    unsigned int fieldElementBits;         /* field element size in bits */
} A_EC_PARAMS;
```

### Format of *info* returned by B\_GetAlgorithmInfo:

B\_GetAlgorithmInfo is not supported with this AI. If called, it will return an error.

## Crypto-C procedures to use with algorithm object:

B\_GenerateI n i t and B\_GenerateKeypai r. B\_GenerateKeypai r sets the *publi cKey* key object with the KI\_EC Pub l i c information and the *pri vateKey* key object with the KI\_EC Pri vate information. You must pass an initialized random algorithm to B\_GenerateKeypai r.

## Algorithm methods to include in application's algorithm chooser:

AM\_ECFP\_KEY\_GEN for odd prime fields and AM\_ECF2POLY\_KEY\_GEN for even characteristic.

## AI\_ECPParameters

### Purpose:

This AI allows you to specify EC parameters to be used for elliptic curve operations. New EC parameters may be generated using the AI\_ECPParamGen algorithm type.

### Type of information this allows you to use:

the parameters generated by executing AI\_ECPParamGen for either generating keys or executing key agreements.

### Format of *info* supplied to B\_SetAlgorithmInfo:

pointer to a A\_EC\_PARAMS structure that has been set by AI\_ECPParamGen:

```
typedef struct {
    unsigned int version;                /* implementation version */
    unsigned int fieldType;             /* indicates type of base field */
    ITEM        fieldInfo;             /* The prime number if fieldType = FT_FP; */
                /* the basis polynomial if fieldType = FT_F2_POLYNOMIAL; */
                /* and the degree of the field if fieldType = FT_F2_ONB */
    ITEM        coeffA;                 /* elliptic curve coefficient */
    ITEM        coeffB;                 /* elliptic curve coefficient */
    ITEM        base;                   /* elliptic curve group generator */
    ITEM        order;                  /* order of subgroup's generating element */
    ITEM        cofactor;              /* the cofactor of the subgroup */
    unsigned int compressIndicator; /* controls field element representation */
    unsigned int fieldElementBits;    /* field element size in bits */
} A_EC_PARAMS;
```

### Format of *info* returned by B\_GetAlgorithmInfo:

pointer to an A\_EC\_PARAMS structure (see above).

### Crypto-C procedures to use with algorithm object:

B\_SetAlgorithmInfo and B\_GetAlgorithmInfo.

### Algorithm methods to include in application's algorithm chooser:

None.

## AI\_ECParmGen

### Purpose:

This AI allows you to generate EC parameters to be used for elliptic curve operations.

### Type of information this allows you to use:

the input parameters for generating an elliptic curve system as defined in X9.62 Draft and IEEE P1363 Draft.

### Format of *info* supplied to B\_SetAlgorithmInfo:

pointer to a B\_EC\_PARAM\_GEN\_PARAMS structure:

```
typedef struct {
    unsigned int version;                /* implementation version */
    unsigned int fieldType;             /* base field for the elliptic curve */
    unsigned int fieldElementBits;     /* length of field element in bits */
    unsigned int compressIndicator;    /* ignored for now */
    unsigned int minOrderBits;        /* minimum size of group generated by base */
    /* input of 0 defaults to fieldElementBits - 7 */
    unsigned int trialDivBound;       /* maximum size of second largest prime */
    /* subgroup of group generated by base */
    /* input of 0 defaults to 255 */
    unsigned int tableLookup;         /* characteristic 2 only. Set if the */
    /* use of precomputed params is desired */
} B_EC_PARAM_GEN_PARAMS;
```

Set the arguments as follows:

Argument	Values	Comments
<i>version</i>	0	Only value currently available; allows growth for future versions
<i>fieldType</i>	FT_FP	odd prime field
	FT_F2_ONB	even characteristic, optimal normal basis
	FT_F2_POLYNOMIAL	even characteristic, polynomial basis

Argument	Values	Comments
<i>compressIndicator</i>	CI_NO_COMPRESS	do not compress the base or public key
	CI_HYBRID	express the base and public key in "hybrid" form; that is, do not compress, but append the compressed $y$ -coordinate, $\tilde{y}_p$ .
<i>fieldElementBits</i>	64 - 384 bits	<i>fieldType</i> = FT_FP or FT_F2_POLYNOMIAL
	65, 66, 69, 74, 81, 82, 83, 86, 89, 90, 95, 98, 99, 100, 105, 106, 113, 119, 130, 131, 134, 135, 138, 146, 148, 155, 158, 162, 172, 173, 174, 178, 179, 180, 183, 186, 189, 191, 194, 196, 209, 210, 221, 226, 230, 231, 233, 239, 243, 245, 251, 254, 261, 268, 270, 273, 278, 281, 292, 293, 299, 303, 306, 309, 316, 323, 326, 329, 330, 338, 346, 348, 350, 354, 359, 371, 372, 375, 378	<i>fieldType</i> = FT_F2_ONB
<i>minOrderBits</i>	0 (recommended); 1 to <i>fieldElementBits</i>	0 tells Crypto-C to choose the value. Note that not all values in the range 1 - <i>fieldElementBits</i> are secure. Must be set to 0 if <i>tableLookup</i> = 1.
<i>trialDivBound</i>	0 (recommended); 1 - 384	0 tells Crypto-C to choose the value. Must be set to 0 if <i>tableLookup</i> = 1.
<i>tableLookup</i>	0 or 1	set to 0 if <i>fieldType</i> = FT_FP set to 0 if <i>fieldType</i> = FT_F2_ONB or FT_F2_POLYNOMIAL, and you want Crypto-C to generate new parameters from scratch. <i>minOrderBits</i> and <i>trialDivBound</i> may be non-zero. set to 1 if <i>fieldType</i> = FT_F2_ONB or FT_F2_POLYNOMIAL, and you want to generate curves using table lookup. Curve generation will be fast, but <i>minOrderBits</i> and <i>trialDivBound</i> must be set to 0.

**Note:** The parameter range given above for *minOrderBits* includes values that are not secure. If you pass 0 for *minOrderBits*, Crypto-C will choose the value for

you. You should only pass a non-zero value if you are certain that you are fully aware of the underlying cryptographic issues.

### Format of *info* returned by `B_GetAlgorithmInfo`:

pointer to a `B_EC_PARAM_GEN_PARAMS` structure (see above).

### Crypto-C procedures to use with algorithm object:

`B_GenerateInit` and `B_GenerateParameters`. `B_GenerateParameters` sets the *resultAlgorithmObject* with the parameter information. You must pass an initialized random algorithm to `B_GenerateParameters`.

### Algorithm methods to include in application's algorithm chooser:

`AM_ECFP_PARAM_GEN` for odd prime fields and `AM_ECF2POLY_PARAM_GEN` for even characteristic.

### Notes:

Generating an elliptic curve for even characteristic without table lookup (*fieldType* = `FT_F2_ONB` or `FT_F2_POLYNOMIAL` and *tableLookup* = 0) can be extremely time-consuming, taking several hours in some cases. In general, larger values for *minOrderBits* mean longer times for curve generation. Therefore, if you wish to generate curves for even characteristic, but do not want to use table lookup, you can speed curve generation by setting a smaller value for *minOrderBits*. Remember, however, that the size of *minOrderBits* is directly tied to the security of your elliptic curve cryptosystem. Setting *minOrderBits* allows you to make a trade-off between the time it takes to generate curves and the security of your system.

## AI\_ECPubKey

### Purpose:

This AI allows you to specify an EC public key and underlying EC parameters in order to build an acceleration table.

### Type of information this allows you to use:

a specified elliptic curve public key to build a public-key specific acceleration table.

### Format of *info* supplied to B\_SetKeyInfo:

pointer to an A\_EC\_PUBLIC\_KEY structure:

```
typedef struct {
    A_EC_PARAMS curveParams;    /* the underlying elliptic curve parameters */
    ITEM pubKey;                /* public component */
} A_EC_PUBLIC_KEY;
```

Each ITEM supplies an integer in canonical format, where the ITEM's *data* points to an unsigned byte array -- most significant byte first -- and the ITEM's *len* gives its length. For all ITEM values except the public component (*x*) and the curve parameter *base*, leading zeros are stripped before they are copied to the key object.

### Format of *info* returned by B\_GetAlgorithmInfo:

pointer to an A\_EC\_PUBLIC\_KEY structure.

### Can get this info type if algorithm object already has:

AI\_ECPubKey.

## AI\_FeedbackCipher

### Purpose:

This AI allows you to perform various kinds of block cipher encryption or decryption with feedback. The parameters of this AI include encryption method, feedback method, and padding method.

### Type of information this allows you to use:

a descriptor for block ciphers with feedback, as defined in X9.52.

### Format of *info* supplied to B\_SetAlgorithmInfo:

a pointer to a B\_BLK\_CIPHER\_W\_FEEDBACK\_PARAMS structure:

```
typedef struct {
    unsigned char *encryptionMethodName;          /* examples include */
                                                    /* "des", "des_ede" */
    POINTER      encryptionParams;              /* e.g., RC5 parameters */
    unsigned char *feedbackMethodName;          /* feedback method name, */
                                                    /* e.g., "cbc" */
    POINTER      feedbackParams;                /* Points at init vector ITEM */
                                                    /* for all feedback modes except cfb */
    unsigned char *paddingMethodName;           /* padding method name, */
                                                    /* e.g., "pad" */
    POINTER      paddingParams;                /* Ignored for now, but may be used */
                                                    /* for new padding schemes */
} B_BLK_CIPHER_W_FEEDBACK_PARAMS;
```

### Format of *info* returned by B\_GetAlgorithmInfo:

pointer to a structure of type B\_BLK\_CIPHER\_W\_FEEDBACK\_PARAMS.

## Type of padding schemes available:

Padding Scheme	Reference String	Comments
Standard CBC padding	"pad"	
No padding	"nopad"	Input length must be a multiple of cipher block length (= 8 for all but rc5-64)
Stream	"stream"	Only available when using CFB in 1-bit and 8-bit modes.

## Crypto-C procedures to use with algorithm object:

B\_EncryptInit, B\_EncryptUpdate, B\_EncryptFinal, B\_DecryptInit, B\_DecryptUpdate, and B\_DecryptFinal. You may pass (B\_ALGORITHM\_OBJ) NULL\_PTR for all *randomAlgorithm* arguments.

## Algorithm methods to include in application's algorithm chooser:

the block cipher AM and the feedback mode AM specified by *encryptionMethodName* and *feedbackMethodName*, respectively.

Table 2-1 Algorithm methods for block ciphers

<i>encryptionMethodName</i>	Algorithm methods to include in chooser	Parameters	Key Size
<b>Encryption</b>			
"des"	AM_DES_ENCRYPT;	null	8 bytes
"des_ede"	AM_DES_EDE_ENCRYPT;	null	24 bytes
"desx"	AM_DESX_ENCRYPT;	null	24 bytes
"rc2"	AM_RC2_ENCRYPT;	Pointer to an A_RC2_PARAMS structure	1 - 128 bytes
"rc5"	AM_RC5_ENCRYPT;	Pointer to an A_RC5_PARAMS structure	0 - 255 bytes; 32-bit word
"rc5_64"	AM_RC5_64ENCRYPT;	Pointer to an A_RC5_PARAMS structure	0 - 255 bytes; 64-bit word
<b>Decryption</b>			
"des"	AM_DES_DECRYPT;	null	8 bytes

Table 2-1 Algorithm methods for block ciphers

<i>encryptionMethodName</i>	Algorithm methods to include in chooser	Parameters	Key Size
"des_eede"	AM_DES_EDE_DECRYPT;	null	24 bytes
"desx"	AM_DESX_DECRYPT;	null	24 bytes
"rc2"	AM_RC2_DECRYPT;	Pointer to an A_RC2_PARAMS structure	1 - 128 bytes
"rc5"	AM_RC5_DECRYPT;	Pointer to an A_RC5_PARAMS structure	0 - 255 bytes; 32-bit word
"rc5_64"	AM_RC5_64DECRYPT; ;	Pointer to an A_RC5_PARAMS structure	0 - 255 bytes; 64-bit word

The RC2 algorithm methods, AM\_RC2\_ENCRYPT and AM\_RC2\_DECRYPT, require an A\_RC2\_PARAMS structure:

```
typedef struct {
    unsigned int effectiveKeyBits;          /* effective key size in bits */
} A_RC2_PARAMS;
```

The RC5 algorithm methods, AM\_RC5\_ENCRYPT, AM\_RC564\_ENCRYPT, AM\_RC5\_DECRYPT, and AM\_RC564\_DECRYPT, require an A\_RC5\_PARAMS structure. Note that the 64-bit versions of RC5, AM\_RC5\_64\_ENCRYPT and AM\_RC5\_64\_DECRYPT, are evaluation implementations and are not optimized in Crypto-C 4.2:

```
typedef struct {
    unsigned int version;    /* currently version 1.0 -- defined as 0x10 */
    unsigned int rounds;    /* number of rounds (0 - 255) */
    unsigned int wordSizeInBits; /* 32 for "rc5" or 64 for "rc5_64" */
} A_RC5_PARAMS;
```

Table 2-2 Algorithm methods for feedback modes

<i>feedbackMethodName</i>	Algorithm methods to include in chooser	Parameter Type
Encryption		
"cbc"	AM_CBC_ENCRYPT;	ITEM that contains the initialization vector

Table 2-2 Algorithm methods for feedback modes

<i>feedbackMethodName</i>	Algorithm methods to include in chooser	Parameter Type
"cbc_i nterl eaved"	AM_CBC_I NTER_L EAVED_ENCRYPT ;	ITEM that contains the initialization vector
"cfb"	AM_CFB_ENCRYPT;	B_CFB_PARAMS
"cfb_pi pel i ned"	AM_CFB_PI PELI NED_ENCRYPT;	B_CFB_PARAMS
"ecb"	AM_ECB_ENCRYPT;	unsigned int that gives the block length
"ofb"	AM_OFB_ENCRYPT;	ITEM that contains the initialization vector
"ofb_pi pel i ned"	AM_OFB_PI PELI NED_ENCRYPT;	ITEM that contains the initialization vector
Decryption		
"cbc"	AM_CBC_DECRYPT;	ITEM that contains the initialization vector
"cbc_i nterl eaved"	AM_CBC_I NTER_L EAVED_DECRYPT ;	ITEM that contains the initialization vector
"cfb"	AM_CFB_DECRYPT;	B_CFB_PARAMS
"cfb_pi pel i ned"	AM_CFB_PI PELI NED_DECRYPT;	B_CFB_PARAMS
"ecb"	AM_ECB_DECRYPT;	unsigned int that gives the block length
"ofb"	AM_OFB_DECRYPT;	ITEM that contains the initialization vector
"ofb_pi pel i ned"	AM_OFB_PI PELI NED_DECRYPT;	ITEM that contains the initialization vector

The CFB modes require a B\_CFB\_PARAMS structure:

```
typedef struct {
    ITEM ivItem;
    unsigned int transferSize;
} B_CFB_PARAMS;
```

**Note:** The initialization vector should be the same size as the block. In particular, the IV should be 8 bytes, except for RC5 implemented with a 64-bit word, which requires a 16-byte IV.

## Key info types for keyObject in B\_EncryptInit or B\_DecryptInit:

Depends on cipher type, as follows:

Cipher	KIs
DES	KI_1tem, KI_DES8, KI_DES8Strong, KI_8Byte
Triple DES	KI_1tem, KI_DES24Strong, KI_24Byte
DESX	KI_1tem, KI_DES24Strong, KI_24Byte
RC2	KI_1tem, KI_8Byte
RC5	KI_1tem, which gives the address and length of the RC5 Key.

## Compatible representations:

Cipher	Compatible representations
DES with CBC mode	AI_DES_CBC_IV8, AI_DES_CBCPadI V8, AI_DES_CBCPadBER, AI_DES_CBCPadPEM, and AI_DES_CBC_BSAFE1
TDES with CBC mode	AI_DES_EDE3_CBC_IV8, AI_DES_EDE3_CBCPadI V8, and AI_DES_EDE3_CBCPadBER
DESX with CBC mode	AI_DESX_CBC_IV8, AI_DESX_CBCPadI V8, AI_DESX_CBCPadBER, and AI_DESX_CBC_BSAFE1
RC2 with CBC mode	AI_RC2_CBC, AI_RC2_CBCPad, AI_RC2_CBCPadBER, and AI_RC2_CBCPadPEM
RC5 with CBC mode and 32-bit word	AI_RC2_CBC_BSAFE1, AI_RC5_CBC, and AI_RC5_CBCPad

## Output considerations:

For encryption, when padding is used, the total number of output bytes can be as many as one block size more than the total input. For decryption, the output buffer should be the same size as the input buffer, even if padding was used.

## AI\_HMAC

### Purpose:

This AI allows you to create a message authentication code using a keyed hashing algorithm called HMAC.

### Type of information this allows you to use:

the specified digest algorithm for performing HMAC (*Hashed-based Message Authentication Code*) as defined in the SET draft standard, a subset of the Draft-IETF-IPSEC-AH-HMAC-SHA-04.

### Format of *info* supplied to B\_SetAlgorithmInfo:

pointer to a B\_DIGEST\_SPECIFIER structure:

```
typedef struct {
    B_INFO_TYPE digestInfoType;
    POINTER digestInfoParams;
} B_DIGEST_SPECIFIER;
```

Crypto-C 4.2 supports AI\_SHA1 and AI\_MD5 as a *digestInfoType*, with NULL\_PTR as the *digestInfoParams*.

### Format of *info* returned by B\_GetAlgorithmInfo:

pointer to a B\_DIGEST\_SPECIFIER structure.

### Crypto-C procedures to use with algorithm object:

B\_DigestInit, B\_DigestUpdate, and B\_DigestFinal. You must pass a key object compatible with KI\_Item with at least one byte of keying material as the *keyObject* argument in B\_DigestInit. It is recommended that minimally 20 bytes of key be used when SHA1 is the hash function. More bytes are recommended if the key bytes are weakly random (low entropy keys).

### Algorithm methods to include in application's algorithm chooser:

The appropriate AM for the digest specified; for instance, AM\_SHA when the *digestInfoType* is AI\_SHA1, and AM\_MD5 for AI\_MD5.

## Output considerations:

The output of `B_DigestFinal` will be the length of the output of the digest specified; for instance, 20 bytes when *digestInfoType* is `AI_SHA1`.

## AI\_HW\_Random



### Purpose:

This AI allows you to generate random bytes using a hardware device.

### Type of information this allows you to use:

random bytes generated by your hardware device.

### Format of *info* supplied to `B_SetAlgorithmInfo`:

`NULL_PTR`.

### Format of *info* returned by `B_GetAlgorithmInfo`:

`NULL_PTR`.

### Crypto-C procedures to use with algorithm object:

`B_RandomInit` and `B_GenerateRandomBytes`, and as the *randomAlgorithm* argument to other procedures.

### Algorithm methods to include in application's algorithm chooser:

`AM_HW_RANDOM`.

### Notes:

Can only be used in conjunction with a hardware implementation; if no hardware implementation is present, `AM_HW_RANDOM` does not do anything. `AM_HW_RANDOM` can only be used if you have called `B_CreateSessionChooser` for your application.

# AI\_KeypairTokenGen



## Purpose:

This AI allows you to generate the token form of a public/private key pair with a hardware device.

## Type of information this allows you to use:

the parameters for generating the token form of a public/private key pair. The BSAFE Hardware API (BHAPI) supports token forms of RSA strong key pair generation as defined in PKCS #1 and DSA key pair generation as defined in FIPS PUB 186.

## Format of *info* supplied to B\_SetAlgorithmInfo:

pointer to an A\_KEYPAIR\_SPECIFIER structure:

```
typedef struct {
    A_KEYPAIR_DEFINDER privateKeyDef;      /* Specifications for private key */
    A_KEYPAIR_DEFINDER publicKeyDef;      /* Specifications for public key */
    POINTER             keyParams;       /* Points to RSA params in RSA case, ie, */
                                                /* A_RSA_KEY_GEN_PARAMS. */
                                                /* Points to DSA params in DSA case. */
    unsigned char      cipherName;       /* String tag for key's cipher class */
                                                /* Either "rsa" or "dsa" to tag */
} A_KEYPAIR_SPECIFIER;
```

where A\_KEYPAIR\_DEFINDER is defined by:

```
typedef struct {
    unsigned int keyUsage;                /* X509 key usage bit map */
    UINT4       lifeTime;               /* Key lifetime; under consideration */
    unsigned int protectFlag;          /* Store key in encrypted form */
} A_KEYPAIR_DEFINDER;
```

## Format of *info* returned by B\_GetAlgorithmInfo:

pointer to an A\_KEYPAIR\_SPECIFIER structure (see above).

## Crypto-C procedures to use with algorithm object:

B\_GenerateInit and B\_GenerateKeypair. If hardware is present, B\_GenerateKeypair sets the *publicKeyDef* and *privateKeyDef* key objects with the public and private key information from KI\_Token. If no hardware is present, and software emulation methods have been included in the hardware chooser, B\_GenerateKeypair sets the *publicKeyDef* and *privateKeyDef* key objects with the public and private key information from KI\_KeypairToken. You must pass an initialized random algorithm to B\_GenerateKeypair, unless the hardware manufacturer has it internally implemented. In this case, a properly cast NULL\_PTR should be used.

## Algorithm methods to include in application's algorithm chooser:

the key-pair generation AM specified by *cipherName*:

<i>cipherName</i>	Algorithm methods to include in chooser
"dsa"	AM_DSA_KEY_TOKEN_GEN
"rsa"	AM_RSA_KEY_TOKEN_GEN

## Notes:

Can only be used in conjunction with a hardware implementation or software emulation; if no hardware implementation is present, AI\_KeypairTokenGen does not do anything. AI\_KeypairTokenGen can only be used if you have called B\_CreateSessionChooser for your application.

The corresponding software-emulation methods passed to B\_CreateSessionChooser via the HARDWARE\_CHOOSER list are a HW\_TABLE\_ENTRY\_SF\_RSA\_KEY\_TOKEN\_GEN for RSA keys and a HW\_TABLE\_ENTRY\_SF\_DSA\_KEY\_TOKEN\_GEN for DSA keys. These provides software support in the case that hardware is unavailable. These methods can be utilized only by including inside the hardware chooser table.

At B\_GenerateInit the key generation object is bound to the hardware device, if one is available. If no hardware device is present, the key-generation object is bound to the software-emulation method if it has been included in the hardware chooser; it defaults to the null method otherwise. For example, for an RSA key token, if no hardware is present, the key generation object is bound to SF\_RSA\_KEY\_TOKEN\_GEN if it is included in the hardware chooser and defaults to AM\_RSA\_KEY\_TOKEN\_GEN otherwise.

## AI\_MAC

### Purpose:

This AI allows you to create a variable-length message authentication code on a non-linear feedback shift register.

### Type of information this allows you to use:

the MAC length parameter for the MAC message authentication code algorithm

### Format of *info* supplied to `B_SetAlgorithmInfo`:

pointer to a `B_MAC_PARAMS` structure:

```
typedef struct {
    unsigned int macLen;           /* length of MAC value */
} B_MAC_PARAMS;
```

The minimum *macLen* is 2.

### Format of *info* returned by `B_GetAlgorithmInfo`:

pointer to a `B_MAC_PARAMS` structure (see above).

### Crypto-C procedures to use with algorithm object:

`B_DigestInit`, `B_DigestUpdate`, and `B_DigestFinal`. Supply `NULL_PTR` for the *keyObject* argument in `B_DigestInit`.

### Algorithm methods to include in application's algorithm chooser:

AM\_MAC.

### Output considerations:

The output of `B_DigestFinal` will be *macLen* bytes long.

## AI\_MD

### Purpose:

Deprecated. This AI is included only for background compatibility.

### Type of information this allows you to use:

the MD message digest algorithm as defined by BSAFE 1.x.

### Format of *info* supplied to B\_SetAlgorithmInfo:

NULL\_PTR.

### Format of *info* returned by B\_GetAlgorithmInfo:

NULL\_PTR.

### Crypto-C procedures to use with algorithm object:

B\_DigestInit, B\_DigestUpdate, and B\_DigestFinal. Supply NULL\_PTR for the *keyObject* argument in B\_DigestInit.

### Algorithm methods to include in application's algorithm chooser:

AM\_MD.

### Output considerations:

The output of B\_DigestFinal will be 16 bytes long.

## AI\_MD2

### Purpose:

This AI allows you to create a message digest using the MD2 digest algorithm as defined in RFC 1319. This algorithm processes input data 16 bytes at a time but the length of the input does not have to be a multiple of 16 as the algorithm pads automatically. The primary use for this AI is to authenticate data. Other algorithms that can be used for message digesting are AI\_MD5 and AI\_SHA1 and their variants. See AI\_MD2\_BER for the MD2 algorithm type with BER encoding. See AI\_MD2\_PEM for the MD2 algorithm type with PEM encoding.

### Type of information this allows you to use:

the MD2 message digest algorithm as defined in RFC 1319.

### Format of *info* supplied to B\_SetAlgorithmInfo:

NULL\_PTR.

### Format of *info* returned by B\_GetAlgorithmInfo:

NULL\_PTR.

### Crypto-C procedures to use with algorithm object:

B\_DigestInit, B\_DigestUpdate, and B\_DigestFinal. Supply NULL\_PTR for the *keyObject* argument in B\_DigestInit.

### Algorithm methods to include in application's algorithm chooser:

AM\_MD2.

### Compatible representation:

AI\_MD2\_BER, AI\_MD2\_PEM.

### Output considerations:

The output of B\_DigestFinal will be 16 bytes long.

## AI\_MD2\_BER

### Purpose:

This AI is similar to AI\_MD2 except that it uses the ASN.1 BER format. This AI allows you to parse and create ASN.1 algorithm identifiers such as used in PKCS #7 and other protocols. You call B\_SetAlgorithmInfo to initialize an algorithm object from the encoded algorithm identifier. You call B\_GetAlgorithmInfo with this AI to create an encoded algorithm identifier from an algorithm object that was created using AI\_MD2, AI\_MD2\_BER or AI\_MD2\_PEM. The OID for this algorithm, excluding the tag and length bytes, in decimal, is "42, 134, 72, 134, 247, 13, 2, 2". Also see AI\_MD2.

### Type of information this allows you to use:

the encoding of an algorithm identifier that specifies the MD2 message digest algorithm as defined in RFC 1319.

### Format of *info* supplied to B\_SetAlgorithmInfo:

pointer to an ITEM structure that gives the address and length of the BER-encoded algorithm identifier. The encoding is converted to DER before it is copied to the algorithm object. B\_SetAlgorithmInfo returns BE\_WRONG\_ALGORITHM\_INFO if the algorithm identifier specifies a message digest algorithm other than MD2.

### Format of *info* returned by B\_GetAlgorithmInfo:

pointer to an ITEM structure that gives the address and length of the DER-encoded algorithm identifier.

### Crypto-C procedures to use with algorithm object:

B\_DigestInit, B\_DigestUpdate, and B\_DigestFinal. Supply NULL\_PTR for the *keyObject* argument in B\_DigestInit.

### Algorithm methods to include in application's algorithm chooser:

AM\_MD2.

### Compatible representation:

AI\_MD2, AI\_MD2\_PEM.

## Output considerations:

The output of `B_DigestFinal` will be 16 bytes long.

## AI\_MD2\_PEM

### Purpose:

This AI is similar to AI\_MD2 except that it uses the PEM format. This AI allows you to parse and create PEM algorithm identifiers such as used in the Privacy Enhanced Mail protocol. You call `B_SetAlgorithmInfo` to initialize an algorithm object from the encoded algorithm identifier. You call `B_GetAlgorithmInfo` with this AI to create an encoded algorithm identifier from an algorithm object that was created using AI\_MD2, AI\_MD2\_BER, or AI\_MD2\_PEM. Also see AI\_MD2.

### Type of information this allows you to use:

an RFC 1423 identifier that specifies the MD2 message digest algorithm as defined in RFC 1319. This algorithm info type is intended to process the digest identifier in a MIC-Info field in a PEM encapsulated header.

### Format of *info* supplied to `B_SetAlgorithmInfo`:

pointer to a null-terminated string (`char *`) that gives the RSA-MD2 identifier. For example, "RSA-MD2." Space and tab characters are removed from the string before it is copied to the algorithm object. `B_SetAlgorithmInfo` returns `BE_WRONG_ALGORITHM_INFO` if the algorithm identifier specifies an identifier other than RSA-MD2.

### Format of *info* returned by `B_GetAlgorithmInfo`:

pointer to a null-terminated string that gives the RSA-MD2 identifier.

### Crypto-C procedures to use with algorithm object:

`B_DigestInit`, `B_DigestUpdate`, and `B_DigestFinal`. Supply `NULL_PTR` for the *keyObject* argument in `B_DigestInit`.

### Algorithm methods to include in application's algorithm chooser:

AI\_MD2.

### Compatible representation:

AI\_MD2, AI\_MD2\_BER.

## Output considerations:

The output of `B_DigestFinal` will be 16 bytes long.

## AI\_MD2Random

### Purpose:

This AI allows you to generate a stream of pseudo-random numbers which are guaranteed to have a very high degree of randomness. Random numbers are used in deriving public and private keys, initialization vectors, etc. This algorithm is the same as AI\_MD5Random described in RSA Labs Bulletin #8 except that the underlying digest algorithm used is MD2 instead of MD5. The details of the AI\_MD5Random algorithm are available online from RSA Laboratories at <http://www.rsa.com/rsalabs/html/bulletins.html>.

Other algorithms that can be used to generate pseudo-random numbers are AI\_MD5Random and AI\_X962Random\_V0.

### Type of information this allows you to use:

the MD2-Random algorithm for generating pseudo-random numbers, as defined by RSA Data Security, Inc.

### Format of *info* supplied to B\_SetAlgorithmInfo:

NULL\_PTR.

### Format of *info* returned by B\_GetAlgorithmInfo:

NULL\_PTR.

### Crypto-C procedures to use with algorithm object:

B\_RandomInit, B\_RandomUpdate, and B\_GenerateRandomBytes, and as the *randomAlgorithm* argument to other procedures.

### Algorithm methods to include in application's algorithm chooser:

AM\_MD2\_RANDOM.

## AI\_MD2WithDES\_CBCPad

### Purpose:

This AI allows you to perform password-based encryption. This means that the input data will be encrypted with a secret key derived from a password, and it can be successfully decrypted only when the correct password is provided. Although this AI can be used to encrypt arbitrary data, its intended primary use is for encrypting private keys when transferring them from one computer system to another, as described in PKCS #8.

This AI employs DES secret-key encryption in cipher-block chaining (CBC) mode with padding, where the secret key is derived from a password using the MD2 message digest algorithm. The details of this algorithm are contained in PKCS #5. DES is defined in FIPS PUB 81, and CBC mode of DES is defined in FIPS PUB 46-1. RFC 1319 describes MD2. Other algorithms that can be used for password-based encryption are AI\_MD5WithDES\_CBCPad, AI\_MD5WithRC2\_CBCPad, AI\_MD2WithRC2\_CBCPad, and AI\_SHA1WithDES\_CBCPad.

### Type of information this allows you to use:

the salt and iteration count for the MD2 With DES-CBC password-based encryption algorithm as defined in PKCS #5.

### Format of *info* supplied to B\_SetAlgorithmInfo:

pointer to a B\_PBE\_PARAMS structure:

```
typedef struct {
    unsigned char *salt;           /* pointer to 8-byte salt value */
    unsigned int  iterationCount; /* iteration count */
} B_PBE_PARAMS;
```

RSA Data Security, Inc. recommends a minimum iteration count of 1,000. However, for an additional byte or two of security the iteration should be  $2^8$  to  $2^{16}$ .

### Format of *info* returned by B\_GetAlgorithmInfo:

pointer to a B\_PBE\_PARAMS structure (see above).

## Crypto-C procedures to use with algorithm object:

B\_EncryptInit, B\_EncryptUpdate, B\_EncryptFinal, B\_DecryptInit, B\_DecryptUpdate, and B\_DecryptFinal. You may pass (B\_ALGORITHM\_OBJ)NULL\_PTR for all *randomAlgorithm* arguments.

## Algorithm methods to include in application's algorithm chooser:

AM\_MD2 and AM\_DES\_CBC\_ENCRYPT for encryption or AM\_DES\_CBC\_DECRYPT for decryption.

## Key info types for *keyObject* in B\_EncryptInit or B\_DecryptInit:

KI\_Item that gives the password.

## Compatible representation:

AI\_MD2WithDES\_CBCPadBER.

## Output considerations:

During encryption, this AI pads the output (which DES requires to be a multiple of 8 bytes long). Thus, the total number of output bytes from encryption can be as many as 8 bytes more than the total output.

## AI\_MD2WithDES\_CBCPadBER

### Purpose:

This AI is similar to AI\_MD2WithDES\_CBCPad except that it uses the ASN.1 BER format. This AI allows you to parse and create ASN.1 algorithm identifiers such as used in PKCS #7 and other protocols. You call B\_SetAlgorithmInfo to initialize an algorithm object from the encoded algorithm identifier that includes the salt and iteration count. You call B\_GetAlgorithmInfo with this AI to create an encoded algorithm identifier from an algorithm object that was created using AI\_MD2WithDES\_CBCPad or AI\_MD2WithDES\_CBCPadBER. The OID for this algorithm, excluding the tag and length bytes, in decimal, is "42, 134, 72, 134, 247, 13, 1, 5, 1". Also see AI\_MD2WithDES\_CBCPad.

### Type of information this allows you to use:

the encoding of an algorithm identifier that specifies the MD2 With DES-CBC password-based encryption algorithm as defined in PKCS #5.

### Format of *info* supplied to B\_SetAlgorithmInfo:

pointer to an ITEM structure that gives the address and length of the BER-encoded algorithm identifier. The encoding is converted to DER before it is copied to the algorithm object. B\_SetAlgorithmInfo returns BE\_WRONG\_ALGORITHM\_INFO if the algorithm identifier specifies an algorithm other than MD2 With DES-CBC.

### Format of *info* returned by B\_GetAlgorithmInfo:

pointer to an ITEM structure that gives the address and length of the DER-encoded algorithm identifier.

### Crypto-C procedures to use with algorithm object:

B\_EncryptInit, B\_EncryptUpdate, B\_EncryptFinal, B\_DecryptInit, B\_DecryptUpdate, and B\_DecryptFinal. You may pass (B\_ALGORITHM\_OBJ)NULL\_PTR for all *randomAlgorithm* arguments.

### Algorithm methods to include in application's algorithm chooser:

AM\_MD2 and AM\_DES\_CBC\_ENCRYPT for encryption or AM\_DES\_CBC\_DECRYPT for decryption.

## Key info types for *keyObject* in B\_EncryptInit or B\_DecryptInit:

KI\_Item that gives the password.

## Compatible representation:

AI\_MD2WithDES\_CBCPad.

## Output considerations:

During encryption, this AI pads the output (which DES requires to be a multiple of 8 bytes long). Thus, the total number of output bytes from encryption can be as many as 8 bytes more than the total output.

## AI\_MD2WithRC2\_CBCPad

### Purpose:

This AI allows you to perform password-based encryption. This means that the input data will be encrypted with a secret key derived from a password, and it can be successfully decrypted only when the correct password is provided. Although this AI can be used to encrypt arbitrary data, its intended primary use is for encrypting private keys when transferring them from one computer system to another, as described in PKCS #8.

This AI employs RC2 block cipher with padding, where the secret key is derived from a password using the MD2 message digest algorithm. MD2 is described in RFC 1319. RC2 is described in RFC 2268. The CBC mode is similar to the one used in RC5-CBC which can be found in RFC 2040. Other algorithms that can be used for password-based encryption are AI\_MD5WithDES\_CBCPad, AI\_MD5WithRC2\_CBCPad, AI\_MD2WithDES\_CBCPad, and AI\_SHA1WithDES\_CBCPad.

### Type of information this allows you to use:

the effective key size, salt, and iteration count for the MD2 With RC2-CBC password-based encryption algorithm, as defined by RSA Data Security, Inc.

### Format of *info* supplied to B\_SetAlgorithmInfo:

pointer to a B\_RC2\_PBE\_PARAMS structure:

```
typedef struct {
    unsigned int  effectiveKeyBits;           /* effective key size in bits */
    unsigned char *salt;                       /* pointer to 8-byte salt value */
    unsigned int  iterationCount;             /* iteration count */
} B_RC2_PBE_PARAMS;
```

This algorithm will accept a maximum of 1024 effective key bits for domestic use and 40 effective key bits for export. RSA Data Security, Inc. recommends a minimum iteration count of 1,000. However, for an additional byte or two of security the iteration should be  $2^8$  to  $2^{16}$ .

### Format of *info* returned by B\_GetAlgorithmInfo:

pointer to a B\_RC2\_PBE\_PARAMS structure (see above).

## Crypto-C procedures to use with algorithm object:

B\_EncryptInit, B\_EncryptUpdate, B\_EncryptFinal, B\_DecryptInit, B\_DecryptUpdate, and B\_DecryptFinal. You may pass (B\_ALGORITHM\_OBJ)NULL\_PTR for all *randomAlgorithm* arguments.

## Algorithm methods to include in application's algorithm chooser:

AM\_MD2 and AM\_RC2\_CBC\_ENCRYPT for encryption or AM\_RC2\_CBC\_DECRYPT for decryption.

## Key info types for *keyObject* in B\_EncryptInit or B\_DecryptInit:

KI\_Item that gives the password.

## Compatible representation:

AI\_MD2WithRC2\_CBCPadBER.

## Output considerations:

During encryption, this AI pads the output. Thus, the total number of output bytes from encryption can be as many as 8 bytes more than the total output.

## AI\_MD2WithRC2\_CBCPadBER

### Purpose:

This AI is similar to AI\_MD2WithRC2\_CBCPad except that it uses the ASN.1 BER format. This AI allows you to parse and create ASN.1 algorithm identifiers such as used in PKCS #7 and other protocols. You call B\_SetAlgorithmInfo to initialize an algorithm object from the encoded algorithm identifier that includes the effective key size, salt and iteration count. You call B\_GetAlgorithmInfo with this AI to create an encoded algorithm identifier from an algorithm object that was created using AI\_MD2WithRC2\_CBCPad or AI\_MD2WithRC2\_CBCPadBER. The OID for this algorithm, excluding the tag and length bytes, in decimal, is "42, 134, 72, 134, 247, 13, 1, 5, 4". Also see AI\_MD2WithRC2\_CBCPad.

### Type of information this allows you to use:

the encoding of an algorithm identifier that specifies the MD2 With RC2-CBC password-based encryption algorithm, as defined by RSA Data Security, Inc.

### Format of *info* supplied to B\_SetAlgorithmInfo:

pointer to an ITEM structure that gives the address and length of the BER-encoded algorithm identifier. The encoding is converted to DER before it is copied to the algorithm object. B\_SetAlgorithmInfo returns BE\_WRONG\_ALGORITHM\_INFO if the algorithm identifier specifies an algorithm other than MD2 With RC2-CBC.

### Format of *info* returned by B\_GetAlgorithmInfo:

pointer to an ITEM structure that gives the address and length of the DER-encoded algorithm identifier.

### Crypto-C procedures to use with algorithm object:

B\_EncryptInit, B\_EncryptUpdate, B\_EncryptFinal, B\_DecryptInit, B\_DecryptUpdate, and B\_DecryptFinal. You may pass (B\_ALGORITHM\_OBJ)NULL\_PTR for all *randomAlgorithm* arguments.

### Algorithm methods to include in application's algorithm chooser:

AM\_MD2 and AM\_RC2\_CBC\_ENCRYPT for encryption or AM\_RC2\_CBC\_DECRYPT for decryption.

### **Key info types for *keyObject* in B\_EncryptInit or B\_DecryptInit:**

Key item that gives the password.

### **Compatible representation:**

AI\_MD2WithRC2\_CBCPad.

### **Output considerations:**

During encryption, this AI pads the output. Thus, the total number of output bytes from encryption can be as many as 8 bytes more than the total output.

## AI\_MD2WithRSAEncryption

### Purpose:

This AI allows you to perform signature operations that involve the MD2 digest algorithm and RSA public key algorithm. The digest of a message is created using the MD2 algorithm and then it is signed using PKCS#1 digital signature algorithm. Other algorithms that can be used for the same purpose are AI\_MD5WithRSAEncryption and AI\_SHA1WithRSAEncryption. See AI\_MD2WithRSAEncryptionBER for the same algorithm type with BER encoding.

### Type of information this allows you to use:

the MD2 With RSA Encryption signature algorithm that uses the MD2 digest algorithm and RSA to create and verify RSA digital signatures as defined in PKCS #1. Note that in order to perform PKCS #1 digital signatures with a 16-byte digest, the RSA key must be at least 360 bits long.

### Format of *info* supplied to B\_SetAlgorithmInfo:

NULL\_PTR.

### Format of *info* returned by B\_GetAlgorithmInfo:

NULL\_PTR.

### Crypto-C procedures to use with algorithm object:

B\_SignInit, B\_SignUpdate, B\_SignFinal, B\_VerifyInit, B\_VerifyUpdate, and B\_VerifyFinal. You may pass (B\_ALGORITHM\_OBJ) NULL\_PTR for all *randomAlgorithm* arguments.

### Algorithm methods to include in application's algorithm chooser:

AM\_MD2, and AM\_RSA\_CRT\_ENCRYPT, AM\_RSA\_CRT\_ENCRYPT\_BLI ND, or AM\_RSA\_ENCRYPT, for signature creation; and AM\_RSA\_DECRYPT for signature verification. AM\_RSA\_CRT\_ENCRYPT\_BLI ND performs blinding to protect against timing attacks, whereas AM\_RSA\_CRT\_ENCRYPT does not.

### Key info types for *keyObject* in `B_SignInit`:

KI\_RSA\_CRT, KI\_PKCS\_RSAPrivate, KI\_PKCS\_RSAPrivateBER, KI\_RSAPrivate or KI\_RSAPrivateBSAFE1. Unless you use KI\_RSA\_CRT for your KI, you must include AM\_RSA\_ENCRYPT in your application's algorithm chooser.

### Key info types for *keyObject* in `B_VerifyInit`:

KI\_RSAPublic, KI\_RSAPublicBER, or KI\_RSAPublicBSAFE1.

### Compatible representation:

AI\_MD2WithRSAEncryptionBER.

### Output considerations:

The *signature* result of `B_SignFinal` will be the same size as the RSA key's modulus.

### Notes:

Although the RSA signature operation is called “encryption” and the verification operation is called “decryption”, the signer uses the digest and the private key and follows the steps needed to decrypt, while the verifier uses the transmitted digest and the public key and follows the steps needed to encrypt.

## AI\_MD2WithRSAEncryptionBER

### Purpose:

This AI is similar to AI\_MD2WithRSAEncryption except that it uses the ASN.1 BER format. This AI allows you to parse and create ASN.1 algorithm identifiers such as used in PKCS #7 and other protocols. You call B\_SetAlgorithmInfo to initialize an algorithm object from the encoded algorithm identifier. You call B\_GetAlgorithmInfo with this AI to create an encoded algorithm identifier from an algorithm object that was created using AI\_MD2WithRSAEncryption or AI\_MD2WithRSAEncryptionBER. The OID for this algorithm, excluding the tag and length bytes, in decimal, is "42, 134, 72, 134, 247, 13, 1, 1, 2". Also see AI\_MD2WithRSAEncryption.

### Type of information this allows you to use:

the encoding of an algorithm identifier that specifies the MD2 With RSA Encryption signature algorithm that uses the MD2 digest algorithm and RSA to create and verify RSA digital signatures as defined in PKCS #1.

Note that in order to perform PKCS #1 digital signatures with a 16-byte digest, the RSA key must be at least 360 bits long.

### Format of *info* supplied to B\_SetAlgorithmInfo:

pointer to an ITEM structure that gives the address and length of the BER-encoded algorithm identifier. The encoding is converted to DER before it is copied to the algorithm object. B\_SetAlgorithmInfo returns BE\_WRONG\_ALGORITHM\_INFO if the algorithm identifier specifies an algorithm other than MD2 With RSA Encryption.

### Format of *info* returned by B\_GetAlgorithmInfo:

pointer to an ITEM structure that gives the address and length of the DER-encoded algorithm identifier.

### Crypto-C procedures to use with algorithm object:

B\_SignInit, B\_SignUpdate, B\_SignFinal, B\_VerifyInit, B\_VerifyUpdate, and B\_VerifyFinal. You may pass (B\_ALGORITHM\_OBJ)NULL\_PTR for all *randomAlgorithm* arguments.

## Algorithm methods to include in application's algorithm chooser:

AM\_MD2, and AM\_RSA\_CRT\_ENCRYPT, AM\_RSA\_CRT\_ENCRYPT\_BLI ND, or AM\_RSA\_ENCRYPT, for signature creation; and AM\_RSA\_DECRYPT for signature verification.

AM\_RSA\_CRT\_ENCRYPT\_BLI ND performs blinding to protect against timing attacks, whereas AM\_RSA\_CRT\_ENCRYPT does not.

## Key info types for *keyObject* in B\_SignInit:

KI\_RSA\_CRT, KI\_PKCS\_RSAPri vate, KI\_PKCS\_RSAPri vateBER, KI\_RSAPri vate or KI\_RSAPri vateBSAFE1. Unless you use KI\_RSA\_CRT for your KI, you must include AM\_RSA\_ENCRYPT in your application's algorithm chooser.

## Key info types for *keyObject* in B\_VerifyInit:

KI\_RSAPubl i c, KI\_RSAPubl i cBER, or KI\_RSAPubl i cBSAFE1.

## Compatible representation:

AI\_MD2Wi thRSAEncrypti on.

## Output considerations:

The *signature* result of B\_Si gnFi nal will be the same size as the RSA key's modulus.

## Notes:

Although the RSA signature operation is called “encryption” and the verification operation is called “decryption”, the signer uses the digest and the private key and follows the steps needed to decrypt, while the verifier uses the transmitted digest and the public key and follows the steps needed to encrypt.

## AI\_MD5

### Purpose:

This AI allows you to create a message digest using the MD5 digest algorithm as defined in RFC 1321. This algorithm processes input data 64 bytes at a time but the length of the input does not have to be a multiple of 64 as the algorithm pads automatically.

The primary use for this AI is to authenticate data. Other algorithms that can be used for message digesting are AI\_MD2 and AI\_SHA1 and their variants.

### Type of information this allows you to use:

the MD5 message digest algorithm as defined in RFC 1321.

### Format of *info* supplied to B\_SetAlgorithmInfo:

NULL\_PTR.

### Format of *info* returned by B\_GetAlgorithmInfo:

NULL\_PTR.

### Crypto-C procedures to use with algorithm object:

B\_DigestInit, B\_DigestUpdate, and B\_DigestFinal. Supply NULL\_PTR for the *keyObject* argument in B\_DigestInit.

### Algorithm methods to include in application's algorithm chooser:

AM\_MD5.

### Compatible representation:

AI\_MD5\_BER, AI\_MD5\_PEM.

### Output considerations:

The output of B\_DigestFinal will be 16 bytes long.

## AI\_MD5\_BER

### Purpose:

This AI is similar to AI\_MD5 except that it uses the ASN.1 BER format. This AI allows you to parse and create ASN.1 algorithm identifiers such as used in PKCS #7 and other protocols. You call B\_SetAlgorithmInfo to initialize an algorithm object from the encoded algorithm identifier. You call B\_GetAlgorithmInfo with this AI to create an encoded algorithm identifier from an algorithm object that was created using AI\_MD5, AI\_MD5\_BER, or AI\_MD5\_PEM. The OID for this algorithm, excluding the tag and length bytes, in decimal is "42, 134, 72, 134, 247, 13, 2, 5".

### Type of information this allows you to use:

the encoding of an algorithm identifier that specifies the MD5 message digest algorithm as defined in RFC 1321.

### Format of *info* supplied to B\_SetAlgorithmInfo:

pointer to an ITEM structure that gives the address and length of the BER-encoded algorithm identifier. The encoding is converted to DER before it is copied to the algorithm object. B\_SetAlgorithmInfo returns BE\_WRONG\_ALGORITHM\_INFO if the algorithm identifier specifies a message digest algorithm other than MD5.

### Format of *info* returned by B\_GetAlgorithmInfo:

pointer to an ITEM structure that gives the address and length of the DER-encoded algorithm identifier.

### Crypto-C procedures to use with algorithm object:

B\_DigestInit, B\_DigestUpdate, and B\_DigestFinal. Supply NULL\_PTR for the *keyObject* argument in B\_DigestInit.

### Algorithm methods to include in application's algorithm chooser:

AM\_MD5.

### Compatible representation:

AI\_MD5, AI\_MD5\_PEM.

## Output considerations:

The output of `B_DigestFinal` will be 16 bytes long.

## AI\_MD5\_PEM

### Purpose:

This AI is similar to AI\_MD5 except that it uses the PEM format. This AI allows you to parse and create PEM algorithm identifiers such as used in Privacy Enhanced Mail protocol. You call B\_SetAlgorithmInfo to initialize an algorithm object from the encoded algorithm identifier. You call B\_GetAlgorithmInfo with this AI to create an encoded algorithm identifier from an algorithm object that was created using AI\_MD5, AI\_MD5\_BER, or AI\_MD5\_PEM.

### Type of information this allows you to use:

an RFC 1423 identifier that specifies the MD5 message digest algorithm as defined in RFC 1321. This algorithm info type is intended to process the digest identifier in a MIC-Info field in a PEM encapsulated header.

### Format of *info* supplied to B\_SetAlgorithmInfo:

pointer to a null-terminated string (char \*) that gives the RSA-MD5 identifier. For example, "Rsa-MD5". Space and tab characters are removed from the string before it is copied to the algorithm object. B\_SetAlgorithmInfo returns BE\_WRONG\_ALGORITHM\_INFO if the algorithm identifier specifies an identifier other than RSA-MD5.

### Format of *info* returned by B\_GetAlgorithmInfo:

pointer to a null-terminated string that gives the RSA-MD5 identifier.

### Crypto-C procedures to use with algorithm object:

B\_DigestInit, B\_DigestUpdate, and B\_DigestFinal. Supply NULL\_PTR for the *keyObject* argument in B\_DigestInit.

### Algorithm methods to include in application's algorithm chooser:

AM\_MD5.

### Compatible representation:

AI\_MD5 and AI\_MD5\_BER.

## Output considerations:

The output of `B_DigestFinal` will be 16 bytes long.

## AI\_MD5Random

### Purpose:

This AI allows you to generate a stream of pseudo-random numbers which are guaranteed to have a very high degree of randomness. Random numbers are used in deriving public and private keys, initialization vectors, etc. This AI uses MD5 as an underlying hashing function. The details of this algorithm are available from RSA Laboratories' Bulletin #8 or online at <http://www.rsa.com/rsalabs/html/bulletins.html>.

Other algorithms that can be used to generate pseudo-random numbers are AI\_MD2Random and AI\_X962Random\_VO.

### Type of information this allows you to use:

the MD5-Random algorithm for generating pseudo-random numbers.

### Format of *info* supplied to B\_SetAlgorithmInfo:

NULL\_PTR.

### Format of *info* returned by B\_GetAlgorithmInfo:

NULL\_PTR.

### Crypto-C procedures to use with algorithm object:

B\_RandomInit, B\_RandomUpdate, and B\_GenerateRandomBytes, and as the *randomAlgorithm* argument to other procedures.

### Algorithm methods to include in application's algorithm chooser:

AM\_MD5\_RANDOM.

## AI\_MD5WithDES\_CBCPad

### Purpose:

This AI allows you to perform password-based encryption. This means that the input data will be encrypted with a secret key derived from a password, and it can be successfully decrypted only when the correct password is provided. Although this AI can be used to encrypt arbitrary data, its intended primary use is for encrypting private keys when transferring them from one computer system to another, as described in PKCS #8.

This AI employs DES secret-key encryption in cipher-block chaining (CBC) mode with padding, where the secret key is derived from a password using the MD5 message digest algorithm. The details of this algorithm are contained in PKCS #5. DES is defined in FIPS PUB 81, and CBC mode of DES is defined in FIPS PUB 46-1. RFC 1321 describes MD5.

Other algorithms that can be used for password-based encryption are AI\_MD2WithDES\_CBCPad, AI\_MD2WithRC2\_CBCPad, AI\_MD5WithRC2\_CBCPad, and AI\_SHA1WithDES\_CBCPad.

### Type of information this allows you to use:

the salt and iteration count for the MD5 With DES-CBC password-based encryption algorithm as defined in PKCS #5. The salt is concatenated with the password before being digested by MD5, and the iteration count specifies how many times the digest needs to be run. The count of 2 indicates that the result of digesting password-and-salt string needs to be run once more through MD5. The first 8 bytes of the final digest become the secret key for the DES cipher after being adjusted for parity as required by FIPS PUB 81, and the last 8 bytes become the initialization vector.

### Format of *info* supplied to B\_SetAlgorithmInfo:

pointer to a B\_PBE\_PARAMS structure:

```
typedef struct {
    unsigned char *salt;                /* pointer to 8-byte salt value */
    unsigned int iterationCount;        /* iteration count */
} B_PBE_PARAMS;
```

RSA Data Security, Inc. recommends a minimum iteration count of 1,000. However,

for an additional byte or two of security the iteration should be  $2^8$  to  $2^{16}$ .

### Format of *info* returned by `B_GetAlgorithmInfo`:

pointer to a `B_PBE_PARAMS` structure (see above).

### Crypto-C procedures to use with algorithm object:

`B_EncryptInit`, `B_EncryptUpdate`, `B_EncryptFinal`, `B_DecryptInit`, `B_DecryptUpdate`, and `B_DecryptFinal`. You may pass `(B_ALGORITHM_OBJ)NULL_PTR` for all *randomAlgorithm* arguments.

### Algorithm methods to include in application's algorithm chooser:

`AM_MD5` and `AM_DES_CBC_ENCRYPT` for encryption or `AM_DES_CBC_DECRYPT` for decryption.

### Key info types for *keyObject* in `B_EncryptInit` or `B_DecryptInit`:

`KI_Item` that gives the password.

### Compatible representation:

`AI_MD5WithDES_CBCPadBER`.

### Output considerations:

During encryption, this AI pads the output (which DES requires to be a multiple of 8 bytes long). Thus, the total number of output bytes from encryption can be as many as 8 bytes more than the total output.

## AI\_MD5WithDES\_CBCPadBER

### Purpose:

This AI is similar to AI\_MD5WithDES\_CBCPad except that it uses the ASN.1 BER format. This AI allows you to parse and create ASN.1 algorithm identifiers such as used in PKCS #7 and other protocols. You call B\_SetAlgorithmInfo to initialize an algorithm object from the encoded algorithm identifier which includes ASN.1 encoding of the B\_PBE\_PARAMS structure defined in the description of AI\_MD5WithDES\_CBCPad. You call B\_GetAlgorithmInfo with this AI to create an encoded algorithm identifier from an algorithm object that was created using AI\_MD5WithDES\_CBCPad or AI\_MD5WithDES\_CBCPad. The OID for this algorithm, excluding the tag and length bytes, in decimal is "42, 134, 72, 134, 247, 13, 1, 5, 3"

### Type of information this allows you to use:

the encoding of an algorithm identifier that specifies the MD5 With DES-CBC password-based encryption algorithm as defined in PKCS #5.

### Format of *info* supplied to B\_SetAlgorithmInfo:

pointer to an ITEM structure that gives the address and length of the BER-encoded algorithm identifier. The encoding is converted to DER before it is copied to the algorithm object. B\_SetAlgorithmInfo returns BE\_WRONG\_ALGORITHM\_INFO if the algorithm identifier specifies an algorithm other than MD5 With DES-CBC.

### Format of *info* returned by B\_GetAlgorithmInfo:

pointer to an ITEM structure that gives the address and length of the DER-encoded algorithm identifier.

### Crypto-C procedures to use with algorithm object:

B\_EncryptInit, B\_EncryptUpdate, B\_EncryptFinal, B\_DecryptInit, B\_DecryptUpdate, and B\_DecryptFinal. You may pass (B\_ALGORITHM\_OBJ)NULL\_PTR for all *randomAlgorithm* arguments.

### Algorithm methods to include in application's algorithm chooser:

AM\_MD5 and AM\_DES\_CBC\_ENCRYPT for encryption or AM\_DES\_CBC\_DECRYPT for decryption.

## Key info types for *keyObject* in B\_EncryptInit or B\_DecryptInit:

KI\_Item that gives the password.

## Compatible representation:

AI\_MD5WithDES\_CBCPad.

## Output considerations:

During encryption, this AI pads the output (which DES requires to be a multiple of 8 bytes long). Thus, the total number of output bytes from encryption can be as many as 8 bytes more than the total output.

## AI\_MD5WithRC2\_CBCPad

### Purpose:

This AI allows you to perform password-based encryption. This means that the input data will be encrypted with a secret key derived from a password, and it can be successfully decrypted only when the correct password is provided. Although this AI can be used to encrypt arbitrary data, its intended primary use is for encrypting private keys when transferring them from one computer system to another, as described in PKCS #8.

This AI employs RC2 block cipher with padding, where the secret key is derived from a password using the MD5 message digest algorithm. MD5 is described in RFC 1321. RC2 is described in RFC 2268. The CBC mode is similar to the one used in RC5-CBC which can be found in RFC 2040.

Other algorithms that can be used for password-based encryption are AI\_MD2WithDES\_CBCPad, AI\_MD2WithRC2\_CBCPad, AI\_MD5WithDES\_CBCPad, and AI\_SHA1WithDES\_CBCPad.

### Type of information this allows you to use:

the effective key size, salt, and iteration count for the MD5 With RC2-CBC password-based encryption algorithm. The salt is concatenated with the password before being processed by MD5, and the iteration count specifies how many times the digest needs to be run. The count of 2 indicates that the result of digesting password-and-salt string needs to be run once more through MD5. The first 8 bytes of the final digest are used as an initialization vector for cipher-block chaining mode, while the last 8 bytes are supplied as the key material to the RC2\_CBCPad algorithm. This algorithm modifies the 64 key bits according to the effectiveKeyBits parameter. RSA Data Security, Inc. recommends using values between 40 and 128 bits for the effectiveKeyBits parameter. Since only 64 bits of key material are supplied to the algorithm, effectiveKeyBits values over 64 bits do not improve security.

## Format of *info* supplied to B\_SetAlgorithmInfo:

pointer to a B\_RC2\_PBE\_PARAMS structure:

```
typedef struct {
    unsigned int  effectiveKeyBits;           /* effective key size in bits */
    unsigned char *salt;                       /* pointer to 8-byte salt value */
    unsigned int  iterationCount;             /* iteration count */
} B_RC2_PBE_PARAMS;
```

This algorithm will accept a maximum of 1024 effective key bits for domestic use and 40 effective key bits for export. RSA Data Security, Inc. recommends a minimum iteration count of 1,000. However, for an additional byte or two of security the iteration should be  $2^8$  to  $2^{16}$ .

## Format of *info* returned by B\_GetAlgorithmInfo:

pointer to a B\_RC2\_PBE\_PARAMS structure (see above).

## Crypto-C procedures to use with algorithm object:

B\_EncryptInit, B\_EncryptUpdate, B\_EncryptFinal, B\_DecryptInit, B\_DecryptUpdate, and B\_DecryptFinal. You may pass (B\_ALGORITHM\_OBJ)NULL\_PTR for all *randomAlgorithm* arguments.

## Algorithm methods to include in application's algorithm chooser:

AM\_MD5 and AM\_RC2\_CBC\_ENCRYPT for encryption or AM\_RC2\_CBC\_DECRYPT for decryption.

## Key info types for *keyObject* in B\_EncryptInit or B\_DecryptInit:

KL\_Item that gives the password.

## Compatible representation:

AI\_MD5WithRC2\_CBCPadBER.

## Output considerations:

During encryption, this AI pads the output. Thus, the total number of output bytes from encryption can be as many as 8 bytes more than the total output.

## AI\_MD5WithRC2\_CBCPadBER

### Purpose:

This AI is similar to AI\_MD5WithRC2\_CBCPad except that it uses the ASN.1 BER format. This AI allows you to parse and create ASN.1 algorithm identifiers such as used in PKCS #7 and other protocols. You call B\_SetAlgorithmInfo to initialize an algorithm object from the encoded algorithm identifier which includes ASN.1 encoding of the B\_RC2\_PBE\_PARAMS structure defined in the description of AI\_MD5WithRC2\_CBCPad. You call B\_GetAlgorithmInfo with this AI to create an encoded algorithm identifier from an algorithm object that was created using AI\_MD5WithRC2\_CBCPad or AI\_MD5WithRC2\_CBCPadBER. The OID for this algorithm, excluding the tag and length bytes, in decimal is "42, 134, 72, 134, 247, 13, 1, 5, 6."

### Type of information this allows you to use:

the encoding of an algorithm identifier that specifies the MD5 With RC2-CBC password-based encryption algorithm.

### Format of *info* supplied to B\_SetAlgorithmInfo:

pointer to an ITEM structure that gives the address and length of the BER-encoded algorithm identifier. The encoding is converted to DER before it is copied to the algorithm object. B\_SetAlgorithmInfo returns BE\_WRONG\_ALGORITHM\_INFO if the algorithm identifier specifies an algorithm other than MD5 With RC2-CBC.

### Format of *info* returned by B\_GetAlgorithmInfo:

pointer to an ITEM structure that gives the address and length of the DER-encoded algorithm identifier.

### Crypto-C procedures to use with algorithm object:

B\_EncryptInit, B\_EncryptUpdate, B\_EncryptFinal, B\_DecryptInit, B\_DecryptUpdate, and B\_DecryptFinal. You may pass (B\_ALGORITHM\_OBJ)NULL\_PTR for all *randomAlgorithm* arguments.

### Algorithm methods to include in application's algorithm chooser:

AM\_MD5 and AM\_RC2\_CBC\_ENCRYPT for encryption or AM\_RC2\_CBC\_DECRYPT for decryption.

## Key info types for *keyObject* in B\_EncryptInit or B\_DecryptInit:

Key item that gives the password.

## Compatible representation:

AI\_MD5WithRC2\_CBCPad.

## Output considerations:

During encryption, this AI pads the output. Thus, the total number of output bytes from encryption can be as many as 8 bytes more than the total output.

## AI\_MD5WithRSAEncryption

### Purpose:

This AI allows you to perform signature operations that involve the MD5 digest algorithm and RSA public key algorithm. The digest of a message is created using the MD5 algorithm and then it is signed using PKCS#1 digital signature algorithm. Other algorithms that can be used for the same purpose are AI\_MD2WithRSAEncryption and AI\_SHA1WithRSAEncryption.

### Type of information this allows you to use:

the MD5 With RSA signature algorithm that uses the MD5 digest algorithm and RSA to create and verify RSA digital signatures as defined in PKCS #1. Note that in order to perform PKCS #1 digital signatures with a 16-byte digest, the RSA key must be at least 360 bits long.

### Format of *info* supplied to B\_SetAlgorithmInfo:

NULL\_PTR.

### Format of *info* returned by B\_GetAlgorithmInfo:

NULL\_PTR.

### Crypto-C procedures to use with algorithm object:

B\_SignInit, B\_SignUpdate, B\_SignFinal, B\_VerifyInit, B\_VerifyUpdate, and B\_VerifyFinal. You may pass (B\_ALGORITHM\_OBJ) NULL\_PTR for all *randomAlgorithm* arguments.

### Algorithm methods to include in application's algorithm chooser:

AM\_MD2, and AM\_RSA\_CRT\_ENCRYPT, AM\_RSA\_CRT\_ENCRYPT\_BLI ND, or AM\_RSA\_ENCRYPT, for signature creation; and AM\_RSA\_DECRYPT for signature verification.

AM\_RSA\_CRT\_ENCRYPT\_BLI ND performs blinding to protect against timing attacks, whereas AM\_RSA\_CRT\_ENCRYPT does not.

### Key info types for *keyObject* in B\_SignInit:

KI\_RSA\_CRT, KI\_PKCS\_RSAPrivate, KI\_PKCS\_RSAPrivateBER, KI\_RSAPrivate or

KI\_RSAPri vateBSAFE1. Unless you use KI\_RSA\_CRT for your KI, you must include AM\_RSA\_ENCRYPT in your application's algorithm chooser.

### Key info types for *keyObject* in B\_VerifyInit:

KI\_RSAPubl i c, KI\_RSAPubl i cBER, or KI\_RSAPubl i cBSAFE1.

### Compatible representation:

AI\_MD5Wi thRSAEncrypti onBER.

### Output considerations:

The *signature* result of B\_Si gnFi nal will be the same size as the RSA key's modulus.

### Notes:

Although the RSA signature operation is called “encryption” and the verification operation is called “decryption”, the signer uses the digest and the private key and follows the steps needed to decrypt, while the verifier uses the transmitted digest and the public key and follows the steps needed to encrypt.

## AI\_MD5WithRSAEncryptionBER

### Purpose:

This AI is similar to AI\_MD5WithRSAEncryption except that it uses the ASN.1 BER format. This AI allows you to parse and create ASN.1 algorithm identifiers such as those used in PKCS #7 and other protocols. You call B\_SetAlgorithmInfo to initialize an algorithm object from the encoded algorithm identifier. You call B\_GetAlgorithmInfo with this AI to create an encoded algorithm identifier from an algorithm object that was created using AI\_MD5WithRSAEncryption or AI\_MD5WithRSAEncryptionBER. The OID for this algorithm, excluding the tag and length bytes, in decimal is "42, 134, 72, 134, 247, 13, 1, 1, 4"

### Type of information this allows you to use:

the encoding of an algorithm identifier that specifies the MD5 With RSA signature algorithm that uses the MD5 digest algorithm and RSA to create and verify RSA digital signatures as defined in PKCS #1.

Note that in order to perform PKCS #1 digital signatures with a 16-byte digest, the RSA key must be at least 360 bits long.

### Format of *info* supplied to B\_SetAlgorithmInfo:

pointer to an ITEM structure that gives the address and length of the BER-encoded algorithm identifier. The encoding is converted to DER before it is copied to the algorithm object. B\_SetAlgorithmInfo returns BE\_WRONG\_ALGORITHM\_INFO if the algorithm identifier specifies an algorithm other than MD5 With RSA Encryption.

### Format of *info* returned by B\_GetAlgorithmInfo:

pointer to an ITEM structure that gives the address and length of the DER-encoded algorithm identifier.

### Crypto-C procedures to use with algorithm object:

B\_SignInit, B\_SignUpdate, B\_SignFinal, B\_VerifyInit, B\_VerifyUpdate, and B\_VerifyFinal. You may pass (B\_ALGORITHM\_OBJ)NULL\_PTR for all *randomAlgorithm* arguments.

## Algorithm methods to include in application's algorithm chooser:

AM\_MD2, and AM\_RSA\_CRT\_ENCRYPT, AM\_RSA\_CRT\_ENCRYPT\_BLI ND, or AM\_RSA\_ENCRYPT, for signature creation; and AM\_RSA\_DECRYPT for signature verification.

AM\_RSA\_CRT\_ENCRYPT\_BLI ND performs blinding to protect against timing attacks, whereas AM\_RSA\_CRT\_ENCRYPT does not.

## Key info types for *keyObject* in B\_SignInit:

KI\_RSA\_CRT, KI\_PKCS\_RSAPri vate, KI\_PKCS\_RSAPri vateBER, KI\_RSAPri vate or KI\_RSAPri vateBSAFE1. Unless you use KI\_RSA\_CRT for your KI, you must include AM\_RSA\_ENCRYPT in your application's algorithm chooser.

## Key info types for *keyObject* in B\_VerifyInit:

KI\_RSAPubl i c, KI\_RSAPubl i cBER, or KI\_RSAPubl i cBSAFE1.

## Compatible representation:

AI\_MD5Wi thRSAEncrypti on.

## Output considerations:

The *signature* result of B\_Si gnFi nal will be the same size as the RSA key's modulus.

## Notes:

Although the RSA signature operation is called “encryption” and the verification operation is called “decryption”, the signer uses the digest and the private key and follows the steps needed to decrypt, while the verifier uses the transmitted digest and the public key and follows the steps needed to encrypt.

## AI\_MD5WithXOR

### Purpose:

This AI is used for encrypting the file keys. This algorithm implements a variant of password-based encryption. The data being encrypted is exclusive-or'ed (XOR'ed) with a secret key derived from a password, and it can be successfully decrypted only when the correct password is provided. Since the secret key is a 128-bit output of MD5 message digest algorithm, the data being encrypted should be no longer than 128 bits. A description of MD5 can be found in RFC 1321.

### Type of information this allows you to use:

the salt and iteration count for the MD5 With “exclusive or” (XOR) password-based encryption algorithm. The salt is concatenated with the password before being digested by MD5, and the iteration count specifies how many times the digest needs to be run. The count of 2 indicates that the result of digesting password-and-salt string needs to be run once more through MD5. The final digest is XOR'ed with the data to obtain the encryption.

### Format of *info* supplied to B\_SetAlgorithmInfo:

pointer to a B\_PBE\_PARAMS structure:

```
typedef struct {
    unsigned char *salt;                /* pointer to 8-byte salt value */
    unsigned int  iterationCount;      /* iteration count */
} B_PBE_PARAMS;
```

### Format of *info* returned by B\_GetAlgorithmInfo:

pointer to a B\_PBE\_PARAMS structure (see above).

### Crypto-C procedures to use with algorithm object:

B\_EncryptInit, B\_EncryptUpdate, B\_EncryptFinal, B\_DecryptInit, B\_DecryptUpdate, and B\_DecryptFinal. You may pass (B\_ALGORITHM\_OBJ) NULL\_PTR for all *randomAlgorithm* arguments.

**Algorithm methods to include in application's algorithm chooser:**

AM\_MD5 and AM\_MD5\_RANDOM.

**Key info types for *keyObject* in B\_EncryptInit or B\_DecryptInit:**

KI\_Item that gives the password.

**Compatible representation:**

AI\_MD5WithXOR\_BER.

## AI\_MD5WithXOR\_BER

### Purpose:

This AI is similar to AI\_MD5WithXOR except that it uses the ASN.1 BER format. This AI allows you to parse and create ASN.1 algorithm identifiers such as used in PKCS #7 and other protocols. You call B\_SetAlgorithmInfo to initialize an algorithm object from the encoded algorithm identifier which includes ASN.1 encoding of the B\_PBE\_PARAMS structure defined in the description of AI\_MD5WithXOR. You call B\_GetAlgorithmInfo with this AI to create an encoded algorithm identifier from an algorithm object that was created using AI\_MD5WithXOR or AI\_MD5WithXOR\_BER. The OID for this algorithm, excluding the tag and length bytes, in decimal is "42, 134, 72, 134, 247, 13, 1, 5, 9."

### Type of information this allows you to use:

the encoding of an algorithm identifier that specifies the MD5 With “exclusive or” (XOR) password-based encryption algorithm, as defined by RSA Data Security, Inc.

### Format of *info* supplied to B\_SetAlgorithmInfo:

pointer to an ITEM structure that gives the address and length of the BER-encoded algorithm identifier. The encoding is converted to DER before it is copied to the algorithm object. B\_SetAlgorithmInfo returns BE\_WRONG\_ALGORITHM\_INFO if the algorithm identifier specifies an algorithm other than MD5 With XOR.

### Format of *info* returned by B\_GetAlgorithmInfo:

pointer to an ITEM structure that gives the address and length of the DER-encoded algorithm identifier.

### Crypto-C procedures to use with algorithm object:

B\_EncryptInit, B\_EncryptUpdate, B\_EncryptFinal, B\_DecryptInit, B\_DecryptUpdate, and B\_DecryptFinal. You may pass (B\_ALGORITHM\_OBJ)NULL\_PTR for all *randomAlgorithm* arguments.

### Algorithm methods to include in application’s algorithm chooser:

AM\_MD5 and AM\_MD5\_RANDOM.

**Key info types for *keyObject* in B\_EncryptInit or B\_DecryptInit:**

Key item that gives the password.

**Compatible representation:**

AI\_MD5WithXOR.

## AI\_PKCS\_OAEP\_RSAPrivate

### Purpose:

This AI allows you to decrypt data using the RSA public-key algorithm with the OAEP padding scheme defined in PKCS #1 v2.0. The OAEP padding scheme prevents a theoretical attack on interactive key-establishment protocols that use PKCS #1 v1.5. The parameters of this algorithm include the hash function, mask generator function, and P source function that are explained below. AI\_PKCS\_RSAPrivate provides the PKCS #1 v1.5 version of the RSA private key decryption algorithm.

AI\_SET\_OAEP\_RSAPrivate provides a different type of OAEP padding scheme defined by the SET specification. See AI\_PKCS\_OAEP\_RSAPrivateBER for the same algorithm type with BER encoding.

### Type of information this allows you to use:

the RSA algorithm for performing private key decryption with OAEP message padding as defined in PKCS #1 v2.0 (DRAFT 1- July 14, 1998). When decrypting, this algorithm decodes the data according to the definition of EME-OAEP-Decode as specified in PKCS #1 v2.0.

### Format of *info* supplied to B\_SetAlgorithmInfo:

either:

NULL\_PTR. The following parameters are employed when NULL\_PTR is specified:

PKCS OAEP RSA PARAMETER	DEFAULT VALUE	DEFAULT PARAMS
hashFunc	"sha1"	empty ITEM
maskGenFunc	"mgf1"	empty ITEM
maskGenFuncUnderlyingAlg	"sha1"	empty ITEM
pSourceFunc	"specifiedParameters"	empty ITEM

or:

a pointer to an A\_PKCS\_OAEP\_PARAMS structure:

```
typedef struct {
    unsigned char*      hashFunc;
    ITEM               hashFuncParams;
    unsigned char*      maskGenFunc;
    ITEM               maskGenFuncParams;
    unsigned char*      maskGenFuncUnderlyingAlg;
    ITEM               maskGenFuncUnderlyingAlgParams;
    unsigned char*      pSourceFunc;
    ITEM               pSourceParams;
} A_PKCS_OAEP_PARAMS;
```

The parameters are as follows:

*hashFunc* determines the digest function. Currently, it may contain a NULL\_PTR or a pointer to the null-terminated ASCII string, "sha1". In both cases SHA1 will become the digest function.

*maskGenFunc* determines the mask generator function. Currently, it may contain a NULL\_PTR or a pointer to the null-terminated ASCII string, "mgf1". In both cases MGF1 will become the mask generator function.

*maskGenFuncUnderlyingAlg* may contain a NULL\_PTR or a pointer to the null-terminated ASCII string, "sha1". In both cases SHA1 will become the underlying algorithm.

*pSourceFunc* is the method for determining the PKCS #1 v2.0 OAEP parameter, P. *pSourceFunc* may contain a NULL\_PTR or a pointer to the null-terminated ASCII string, "specifiedParameters". In both cases "specifiedParameters" will become the pSource method.

If *pSourceFunc* is "specifiedParameters" and if *pSourceParams.Len* is 0, then P is assumed to be empty. *pSourceParams* may also be initialized to the caller's data as in this example:

```
pSourceParams.Len = sizeof(dataObject);
pSourceParams.data = &dataObject;
```

*hashFuncParams*, *maskGenFuncParams*, and *maskGenFuncUnderlyingAlgParams* are available to provide for future growth. The caller should initialize these parameters as ITEM types as follows:

```

hashFuncParams.l en = 0;
hashFuncParams.data = NULL_PTR
maskGenFuncParams.l en = 0;
maskGenFuncParams.data = NULL_PTR
maskGenFuncUnderl yingAl gParams.l en = 0;
maskGenFuncUnderl yingAl gParams.data = NULL_PTR

```

Failure to properly initialize these parameters may cause bugs when they are implemented in future versions of Crypto-C. In this case, the default parameters for *pSourceParams* should be set by the caller as follows:

```

pSourceParams.l en = 0;
pSourceParams.data = NULL_PTR;

```

## Format of *info* supplied to B\_GetAlgorithmInfo:

NULL\_PTR.

## Crypto-C procedures to use with algorithm object:

B\_DecryptI nit, B\_DecryptUpdate, and B\_DecryptFi nal . You may pass (B\_ALGORI THM\_OBJ) NULL\_PTR for the *randomAl gori thm* argument in B\_DecryptUpdate and B\_DecryptFi nal .

## Algorithm methods to include in application's algorithm chooser:

AM\_RSA\_CRT\_DECRYPT or AM\_RSA\_CRT\_DECRYPT\_BLI ND for decryption. AM\_RSA\_CRT\_DECRYPT\_BLI ND performs blinding to protect against timing attacks, whereas AM\_RSA\_CRT\_DECRYPT does not. AM\_SHA is required for the default *pSource* digest function. It is also required for MGF1 as underlying algorithm.

## Key info types for keyObject in B\_EncryptI nit or B\_DecryptI nit:

KI\_RSA\_CRT, KI\_PKCS\_RSAPri vate, or KI\_PKCS\_RSAPri vateBER.

## Compatible representation:

AI\_PKCS\_OAEP\_RSAPri vateBER.

## Output considerations:

The output of decryption will be the same size as the original message.

---

## AI\_PKCS\_OAEP\_RSAPrivateBER

### Purpose:

This AI is similar to AI\_PKCS\_OAEP\_RSAPrivate except that it uses the ASN.1 BER format. This AI allows you to parse and create ASN.1 algorithm identifiers such as those used in PKCS #7 and other protocols. You call B\_SetAlgorithmInfo to initialize an algorithm object from the encoded algorithm identifier that includes the hash function, mask generator function, and P source function. You call B\_GetAlgorithmInfo with this AI to create an encoded algorithm identifier from an algorithm object that was created using AI\_PKCS\_OAEP\_RSAPrivate or AI\_PKCS\_OAEP\_RSAPrivateBER. The OID for the RSA OAEP encryption, excluding the tag and length bytes, in decimal, is "42, 134, 72, 134, 247, 13, 1, 1, 7". The OID for the mask function, excluding the tag and length bytes, in decimal, is "42, 134, 72, 134, 247, 13, 1, 1, 8". The OID for the P source function, excluding the tag and length bytes, in decimal, is "42, 134, 72, 134, 247, 13, 1, 1, 9". Also see AI\_PKCS\_OAEP\_RSAPrivate.

### Type of information this allows you to use:

the RSA algorithm for performing private key decryption with OAEP message padding as defined in PKCS #1 v2.0 (DRAFT 1- July 14, 1998). When decrypting, this algorithm decodes the data according to the definition of EME-OAEP-Decode as specified in PKCS #1 v2.0.

### Format of *info* supplied to B\_SetAlgorithmInfo:

pointer to an ITEM structure that gives the address and length of the BER-encoded algorithm identifier. The encoding is converted to DER before it is copied to the algorithm object. B\_SetAlgorithmInfo returns BE\_WRONG\_ALGORITHM\_INFO if the algorithm identifier specifies an algorithm other than RSAES-OAEP Encryption as specified by PKCS #1 v2.0.

The general ASN.1 syntax for RSAES-OAEP is complicated. The simple DER encoding of the default algorithm is given first, followed by the general syntax.

Simple DER encoding for the default algorithm:

```

-- Default Algorithm Identifier for RSAES-OAEP.
-- The DER Encoding of this is in hexadecimal given below.
-- Notice that the DER encoding of the default parameters
-- is just an empty sequence.
-- 30 0D
--   06 09
--     2A 86 48 86 F7 0D 01 01 07
--   30 00
RSAES-OAEP-Default-Identifier ::= AlgorithmIdentifier {
  id-RSAES-OAEP,
  { sha1Identifier,
    mgf1SHA1Identifier,
    pSpecifiedEmptyIdentifier
  }
}

```

The general syntax is:

```

RSAES-OAEP ::= Sequence {
  algorithm      OBJECT IDENTIFIER (id-RSAES-OAEP),
  parameters     RSAES-OAEP-params
}
-- Identifier for PKCS #1 v2.0 OAEP.
-- The DER for this in hexadecimal is:
-- 06 09
--   2A 86 48 86 F7 0D 01 01 07
--
id-RSAES-OAEP OBJECT IDENTIFIER ::= {
  iso(1) member-body(2) us(840) rsads(113549)
  pkcs(1) pkcs-1(1) RSAES-OAEP(7)}
-- Identifier for the PKCS #1 v2.0 mask generation function,
-- which takes a hash function AlgID as a parameter.
-- The DER for this in hexadecimal is:
-- 06 09
--   2A 86 48 86 F7 0D 01 01 08
--
id-mgf1 OBJECT IDENTIFIER ::= {
  iso(1) member-body(2) us(840) rsads(113549)
  pkcs(1) pkcs-1(1) mgf1(8)}

```

```

-- The identifier says that the algorithm by which the P
-- string for RSAES-OAEP is generated is by setting it
-- equal to the contents of the OCTET STRING which is
-- the parameter for this AlgorithmIdentifier.
-- The DER for this in hexadecimal is:
-- 06 09
-- 2A 86 48 86 F7 0D 01 01 09
--
id-pSpecified OBJECT IDENTIFIER ::= {
    iso(1) member-body(2) us(840) rsads(113549)
    pkcs(1) pkcs-1(1) pSpecified(9)}
-- Identifier for the SHA1 digest function.
-- The DER for this in hexadecimal is:
-- 06 05
-- 2B 0E 03 02 1A
--
id-sha1 OBJECT IDENTIFIER ::= {
    iso(1) identified-organization(3) oiw(14) secsig(3)
    algorithms(2) sha1(26) }
-- Syntax of AlgorithmIdentifier.parameters for RSAES-OAEP.
-- Note that the tags in this Sequence are explicit.
-- The DER encoding of DEFAULT values is to omit them.
--
RSAES-OAEP-params ::= SEQUENCE {
    hashFunc          [0] AlgorithmIdentifier {
        {oaepDigestAlgorithms} }
        DEFAULT sha1Identifier,
    maskGenFunc       [1] AlgorithmIdentifier {
        {pkcs1MGFAlgorithms} }
        DEFAULT mgf1SHA1Identifier,
    pSourceFunc       [2] AlgorithmIdentifier {
        {pkcs1PGenAlgorithms} }
        DEFAULT pSpecifiedEmptyIdentifier
}
-- Algorithm Identifier for SHA1, which is the OAEP default.
--
sha1Identifier ::= AlgorithmIdentifier {
    id-sha1, NULL }
-- Default AlgorithmIdentifier for id-RSAES-OAEP.maskGenFunc.
--
mgf1SHA1Identifier ::= AlgorithmIdentifier {
    id-mgf1, sha1Identifier }

```

```

-- This identifier means that P is an empty string, so the digest
_D_ "D
-- of the empty string appears in the RSA block before masking.
--
safe-00.1'D
pSpecifiedEmptyIdentifier ::= AlgorithmIdentifier {
    id-pSpecified, OCTET STRING SIZE (0)
}

```

## Format of *info* supplied to B\_GetAlgorithmInfo:

pointer to an ITEM structure that gives the address and length of the DER-encoded algorithm identifier.

## Crypto-C procedures to use with algorithm object:

The following procedures perform OAEP padding with encryption:

B\_DecryptInit, B\_DecryptUpdate, and B\_DecryptFinal. You may pass (B\_ALGORITHM\_OBJ) NULL\_PTR for the *randomAlgorithm* argument in B\_DecryptUpdate and B\_DecryptFinal.

## Algorithm methods to include in application's algorithm chooser:

AM\_RSA\_CRT\_DECRYPT or AM\_RSA\_CRT\_DECRYPT\_BLIND for decryption. AM\_RSA\_CRT\_DECRYPT\_BLIND performs blinding to protect against timing attacks, whereas AM\_RSA\_CRT\_DECRYPT does not. AM\_SHA is required for the default *pSource* digest function. It is also required for MGF1 as underlying algorithm.

## Key info types for keyObject in B\_EncryptInit or B\_DecryptInit:

KI\_RSA\_CRT, KI\_PKCS\_RSAPrivate, or KI\_PKCS\_RSAPrivateBER.

## Compatible representation:

AI\_PKCS\_OAEP\_RSAPrivate.

## Output considerations:

The output of decryption will be the same size as the original message.

## AI\_PKCS\_OAEP\_RSAPublic

### Purpose:

This AI allows you to encrypt data using the RSA public-key algorithm with the OAEP padding scheme defined in PKCS #1 v2.0. The OAEP padding scheme prevents a theoretical attack on interactive key-establishment protocols that use PKCS #1 v1.5. The parameters of this algorithm include the hash function, mask generator function and P source function that are explained below. AI\_PKCS\_RSAPublic provides the PKCS #1 v1.5 version of the RSA public key encryption algorithm.

AI\_SET\_OAEP\_RSAPublic provides a different type of OAEP padding scheme defined by the SET specification. See AI\_PKCS\_OAEP\_RSAPublicBER for the same algorithm type with BER encoding.

### Type of information this allows you to use:

the RSA algorithm for performing public key encryption with OAEP message padding as defined in PKCS #1 v2.0 (DRAFT 1- July 14, 1998). When encrypting, this algorithm encodes the data according to the definition of EME-OAEP-Encode as specified in PKCS #1 v2.0.

### Format of *info* supplied to B\_SetAlgorithmInfo:

either:

NULL\_PTR. The following parameters are employed when NULL\_PTR is specified:

PKCS OAEP RSA PARAMETER	DEFAULT VALUE	DEFAULT PARAMETERS
hashFunc	"sha1"	empty ITEM
maskGenFunc	"mgf1"	empty ITEM
maskGenFuncUnderlyingAlg	"sha1"	empty ITEM
pSourceFunc	"specifiedParameters"	empty ITEM

or:

a pointer to an A\_PKCS\_OAEP\_PARAMS structure:

```
typedef struct {
    unsigned char*      hashFunc;
    ITEM               hashFuncParams;
    unsigned char*      maskGenFunc;
    ITEM               maskGenFuncParams;
    unsigned char*      maskGenFuncUnderlyingAlg;
    ITEM               maskGenFuncUnderlyingAlgParams;
    unsigned char*      pSourceFunc;
    ITEM               pSourceParams;
} A_PKCS_OAEP_PARAMS;
```

The parameters are as follows:

*hashFunc* determines the digest function. Currently, it may contain a NULL\_PTR or a pointer to the null-terminated ASCII string, "sha1". In both cases SHA1 will become the digest function.

*maskGenFunc* determines the mask generator function. Currently, it may contain a NULL\_PTR or a pointer to the null-terminated ASCII string, "mgf1". In both cases MGF1 will become the mask generator function.

*maskGenFuncUnderlyingAlg* may contain a NULL\_PTR or a pointer to the null-terminated ASCII string, "sha1". In both cases SHA1 will become the underlying algorithm.

*pSourceFunc* is the method for determining the PKCS #1 v2.0 OAEP parameter, P. *pSourceFunc* may contain a NULL\_PTR or a pointer to the null-terminated ASCII string, "specifiedParameters". In both cases "specifiedParameters" will become the pSource method.

If *pSourceFunc* is "specifiedParameters" and if *pSourceParams.Len* is 0, then P is assumed to be empty. *pSourceParams* may also be initialized to the caller's data as in this example:

```
pSourceParams.Len = sizeof(dataObject);
pSourceParams.data = &dataObject;
```

*hashFuncParams*, *maskGenFuncParams*, and *maskGenFuncUnderlyingAlgParams* are available to provide for future growth. The caller should initialize these parameters as ITEM types as follows:

```

hashFuncParams.Len = 0;
hashFuncParams.data = NULL_PTR
maskGenFuncParams.Len = 0;
maskGenFuncParams.data = NULL_PTR
maskGenFuncUnderlyingAl gParams.Len = 0;
maskGenFuncUnderlyingAl gParams.data = NULL_PTR

```

Failure to properly initialize these parameters may cause bugs when they are implemented in future versions of Crypto-C. In this case, the default parameters for *pSourceParams* should be set by the caller as follows:

```

pSourceParams.Len = 0;
pSourceParams.data = NULL_PTR;

```

## Format of *info* supplied to B\_GetAlgorithmInfo:

NULL\_PTR.

## Crypto-C procedures to use with algorithm object:

B\_EncryptInit, B\_EncryptUpdate, and B\_EncryptFinal.

B\_EncryptFinal requires a valid random number generator as a B\_ALGORITHM\_OBJ in its *randomAlgorithm* argument. PKCS #1 v2.0 does not specify the random number generation method. It is recommended that AI\_X962Random\_V0 or AI\_SHA1Random be initialized with enough seed bytes to produce 160 bits of entropy.

You may pass (B\_ALGORITHM\_OBJ)NULL\_PTR for the *randomAlgorithm* argument in B\_EncryptUpdate.

## Algorithm methods to include in application's algorithm chooser:

AM\_RSA\_ENCRYPT.

AM\_SHA is required for the default *pSource* digest function and also for the default MGF underlying digest method.

## Key info types for keyObject in B\_EncryptInit or B\_DecryptInit:

KI\_RSAPublic or KI\_RSAPublicBER.

## Compatible representation:

AI\_PKCS\_RSAPublic in cBER.

## Input constraints:

The key's modulus must be at least  $[(2 * hLen) + 2]$  bytes longer than the message.

## Output considerations:

The output of encryption will be the same size as the key's modulus.

## AI\_PKCS\_OAEP\_RSAPublicBER

### Purpose:

This AI is similar to AI\_PKCS\_OAEP\_RSAPublicBER except that it uses the ASN.1 BER format. This AI allows you to parse and create ASN.1 algorithm identifiers such as those used in PKCS #7 and other protocols. You call B\_SetAlgorithmInfo to initialize an algorithm object from the encoded algorithm identifier that includes the hash function, mask generator function, and P source function. You call B\_GetAlgorithmInfo with this AI to create an encoded algorithm identifier from an algorithm object that was created using AI\_PKCS\_OAEP\_RSAPublicBER or AI\_PKCS\_OAEP\_RSAPublicBER. The OID for the RSA OAEP encryption, excluding the tag and length bytes, in decimal, is "42, 134, 72, 134, 247, 13, 1, 1, 7". The OID for the mask function, excluding the tag and length bytes, in decimal, is "42, 134, 72, 134, 247, 13, 1, 1, 8". The OID for the P source function, excluding the tag and length bytes, in decimal, is "42, 134, 72, 134, 247, 13, 1, 1, 9". Also see AI\_PKCS\_OAEP\_RSAPublicBER.

### Type of information this allows you to use:

the RSA algorithm for performing public key encryption with OAEP message padding as defined in PKCS #1 v2.0 (DRAFT 1- July 14, 1998). When encrypting, this algorithm encodes the data according to the definition of EME-OAEP-Encode as specified in PKCS #1 v2.0.

### Format of *info* supplied to B\_SetAlgorithmInfo:

pointer to an ITEM structure that gives the address and length of the BER-encoded algorithm identifier. The encoding is converted to DER before it is copied to the algorithm object. B\_SetAlgorithmInfo returns BE\_WRONG\_ALGORITHM\_INFO if the algorithm identifier specifies an algorithm other than RSAES-OAEP Encryption as specified by PKCS #1 v2.0.

The general ASN.1 syntax for RSAES-OAEP is complicated. Here the simple DER

encoding of the default algorithm is given first, followed by the general syntax.

```
-- Default Algorithm Identifier for RSAES-OAEP.
-- The DER Encoding of this is in hexadecimal given below.
-- Notice that the DER encoding of the default parameters
-- is just an empty sequence.
-- 30 0D
--   06 09
--     2A 86 48 86 F7 0D 01 01 07
--   30 00
--
-- RSAES-OAEP-Default-Identifier ::= AlgorithmIdentifier {
--   id-RSAES-OAEP,
--   { sha1Identifier,
--     mgf1SHA1Identifier,
--     pSpecifiedEmptyIdentifier
--   }
-- }
```

The general syntax is:

```
RSAES-OAEP ::= Sequence {
  algorithm    OBJECT IDENTIFIER (id-RSAES-OAEP),
  parameters   RSAES-OAEP-params
}
-- Identifier for PKCS #1 v2.0 OAEP.
-- The DER for this in hexadecimal is:
-- 06 09
--   2A 86 48 86 F7 0D 01 01 07
--
id-RSAES-OAEP OBJECT IDENTIFIER ::= {
  iso(1) member-body(2) us(840) rsadsi (113549)
  pkcs(1) pkcs-1(1) RSAES-OAEP(7)}
```

```

-- Identifier for the PKCS #1 v2.0 mask generation function,
-- which takes a hash function AlgID as a parameter.
-- The DER for this in hexadecimal is:
-- 06 09
--   2A 86 48 86 F7 0D 01 01 08
--
id-mgf1 OBJECT IDENTIFIER ::= {
    iso(1) member-body(2) us(840) rsadsi(113549)
    pkcs(1) pkcs-1(1) mgf1(8)}
-- The identifier says that the algorithm by which the P
-- string for RSAES-OAEP is generated is by setting it
-- equal to the contents of the OCTET STRING which is
-- the parameter for this AlgorithmIdentifier.
-- The DER for this in hexadecimal is:
-- 06 09
--   2A 86 48 86 F7 0D 01 01 09
--
id-pSpecified OBJECT IDENTIFIER ::= {
    iso(1) member-body(2) us(840) rsadsi(113549)
    pkcs(1) pkcs-1(1) pSpecified(9)}
-- Identifier for the SHA1 digest function.
-- The DER for this in hexadecimal is:
-- 06 05
--   2B 0E 03 02 1A
--
id-sha1 OBJECT IDENTIFIER ::= {
    iso(1) identified-organization(3) oiw(14) secsig(3)
    algorithms(2) sha1(26) }
-- Syntax of AlgorithmIdentifier parameters for RSAES-OAEP.
-- Note that the tags in this Sequence are explicit.
-- The DER encoding of DEFAULT values is to omit them.
--
RSAES-OAEP-params ::= SEQUENCE {
    hashFunc          [0] AlgorithmIdentifier {
        {oaepDigestAlgorithms} }
        DEFAULT sha1Identifier,
    maskGenFunc       [1] AlgorithmIdentifier {
        {pkcs1MGFAlgorithms} }
        DEFAULT mgf1SHA1Identifier,
    pSourceFunc       [2] AlgorithmIdentifier {
        {pkcs1PGenAlgorithms} }
        DEFAULT pSpecifiedEmptyIdentifier
}

```

```

-- Algorithm Identifier for SHA1, which is the OAEP default.
--
sha1Identifier ::= AlgorithmIdentifier {
    id-sha1, NULL }
-- Default AlgorithmIdentifier for id-RSAES-OAEP.maskGenFunc.
--
mgf1SHA1Identifier ::= AlgorithmIdentifier {
    id-mgf1, sha1Identifier }
-- This identifier means that P is an empty string, so the digest
-- of the empty string appears in the RSA block before masking.
--
pSpecifiedEmptyIdentifier ::= AlgorithmIdentifier {
    id-pSpecified, OCTET STRING SIZE (0)
}

```

## Format of *info* supplied to B\_GetAlgorithmInfo:

pointer to an ITEM structure that gives the address and length of the DER-encoded algorithm identifier.

## Crypto-C procedures to use with algorithm object:

B\_EncryptInit, B\_EncryptUpdate, and B\_EncryptFinal.

B\_EncryptFinal requires a valid random number generator as a B\_ALGORITHM\_OBJ in its *randomAlgorithm* argument. PKCS #1 v2.0 does not specify the random number generation method. It is recommended that AI\_X962Random\_V0 or AI\_SHA1Random be initialized with enough seed bytes to produce 160 bits of entropy.

You may pass (B\_ALGORITHM\_OBJ)NULL\_PTR for the *randomAlgorithm* argument in B\_EncryptUpdate.

## Algorithm methods to include in application's algorithm chooser:

AM\_RSA\_ENCRYPT.

AM\_SHA is required for the default *pSource* digest function and also for the default MGF underlying digest method.

## Key info types for keyObject in B\_EncryptInit or B\_DecryptInit:

KI\_RSAPublic and KI\_RSAPublicBER may be used to perform RSA encryption or decryption.

**Compatible representation:**

AI\_PKCS\_OAEP\_RSAPublic.

**Input constraints:**

The key's modulus must be at least  $[(2 * hLen) + 2]$  bytes longer than the message.

**Output considerations:**

The output of encryption will be the same size as the key's modulus.

## AI\_PKCS\_OAEPRecode



### Purpose:

This AI allows you to perform raw or hardware-based encoding or decoding using the PKCS #1 v2.0 OAEP padding scheme. The OAEP padding scheme prevents a theoretical attack on interactive key-establishment protocols that use PKCS #1 v1.5. The parameters of this algorithm include the hash function, mask generator function, and P source function that are explained below. Encrypting with the AI\_PKCS\_OAEP\_RSAPublic algorithm is equivalent to first encoding the data with AI\_PKCS\_OAEPRecode using the B\_Encode routines and then encrypting with AI\_RSAPublic using the B\_Encrypt routines. See AI\_PKCS\_OAEPRecodeBER for the same algorithm type with BER encoding.

### Type of information this allows you to use:

OAEP message padding as defined in PKCS #1 v2.0 (DRAFT 1- July 14, 1998). When encoding, this algorithm encodes the data according to the definition of EME-OAEP-Encode as specified in PKCS #1 v2.0. When decoding, this algorithm decodes the data according to the definition of EME-OAEP-Decode. This permits the use of raw or hardware-based RSA with the PKCS #1 v2.0 flavor of Optimal Asymmetric Encryption Padding.

### Format of *info* supplied to B\_SetAlgorithmInfo:

Either:

NULL\_PTR.

The following parameters are employed when NULL\_PTR is specified:

PKCS OAEP RSA PARAMETER	DEFAULT VALUE	DEFAULT PARAMETERS
hashFunc	"sha1"	empty ITEM
maskGenFunc	"mgf1"	empty ITEM
maskGenFuncUnderlyingAlg	"sha1"	empty ITEM
pSourceFunc	"specifiedParameters"	empty ITEM

or:

a pointer to an A\_PKCS\_OAEP\_PARAMS structure:

```
typedef struct {
    unsigned char*      hashFunc;
    ITEM                hashFuncParams;
    unsigned char*      maskGenFunc;
    ITEM                maskGenFuncParams;
    unsigned char*      maskGenFuncUnderlyingAlg;
    ITEM                maskGenFuncUnderlyingAlgParams;
    unsigned char*      pSourceFunc;
    ITEM                pSourceParams;
} A_PKCS_OAEP_PARAMS;
```

The parameters are as follows:

*hashFunc* determines the digest function. Currently, it may contain a NULL\_PTR or a pointer to the null-terminated ASCII string, "sha1". In both cases SHA1 will become the digest function.

*maskGenFunc* determines the mask generator function. Currently, it may contain a NULL\_PTR or a pointer to the null-terminated ASCII string, "mgf1". In both cases MGF1 will become the mask generator function.

*maskGenFuncUnderlyingAlg* may contain a NULL\_PTR or a pointer to the null-terminated ASCII string, "sha1". In both cases SHA1 will become the underlying algorithm.

*pSourceFunc* is the method for determining the PKCS #1 v2.0 OAEP parameter, P. *pSourceFunc* may contain a NULL\_PTR or a pointer to the null-terminated ASCII string, "specifiedParameters". In both cases "specifiedParameters" will become the pSource method.

If *pSourceFunc* is "specifiedParameters" and if *pSourceParams.Len* is 0, then P is assumed to be empty. *pSourceParams* may also be initialized to the caller's data as in this example:

```
pSourceParams.Len = sizeof(dataObject);
pSourceParams.data = &dataObject;
```

*hashFuncParams*, *maskGenFuncParams*, and *maskGenFuncUnderlyingAlgParams* are available to provide for future growth. The caller should initialize these parameters as ITEM types as follows:

```
hashFuncParams.l en = 0;
hashFuncParams.data = NULL_PTR
maskGenFuncParams.l en = 0;
maskGenFuncParams.data = NULL_PTR
maskGenFuncUnderl yi ngAl gParams.l en = 0;
maskGenFuncUnderl yi ngAl gParams.data = NULL_PTR
```

Failure to properly initialize these parameters may cause bugs when they are implemented in future versions of Crypto-C. In this case, the default parameters for *pSourceParams* should be set by the caller as follows:

```
pSourceParams.l en = 0;
pSourceParams.data = NULL_PTR;
```

## Format of *info* supplied to **B\_GetAlgorithmInfo**:

NULL\_PTR.

## Crypto-C procedures to use with algorithm object:

**B\_Encode** ni t, **B\_EncodeUpdate**, **B\_EncodeFi nal** , **B\_Decode** ni t, **B\_DecodeUpdate**, and **B\_DecodeFi nal** .

The final call to **B\_EncodeUpdate** does not contain message data. Rather, the trailing call to **B\_EncodeUpdate** is included to pass in a number of random seed bytes for the OAEP encoding process. It is recommended that the caller use **AI\_X962Random\_V0** or **AI\_SHA1Random** to generate *hLen* bytes initialized with 160 bits of entropy. The default digest algorithm for PKCS #1 v2.0 OAEP is SHA1. SHA1 produces a digest of 20 bytes, so *hLen* for SHA1 is 20 bytes.

**B\_Decode\_Update** does not contain an extra call for seed bytes.

## Algorithm methods to include in application's algorithm chooser:

**AM\_SHA** is required for the default *pSource* digest function and also for the default MGF underlying digest method.

## Compatible representation:

**AI\_PKCS\_OAEPRecodeBER**.

**Input constraints:**

The total number of bytes to encode must be at least  $[(2 * hLen) + 1]$  bytes long.

**Output considerations:**

The output of encoding will be an encoded message that is the same size as *maxPartOutLen*. (See `B_EncodeUpdate`, `B_EncodeFinal`, `B_DecodeUpdate`, and `B_DecodeFinal`.) The output of the decoding will be the original message.

---

## AI\_PKCS\_OAEPRecodeBER



### Purpose:

This AI is similar to AI\_PKCS\_OAEPRecode except that it uses the ASN.1 BER format. This AI allows you to parse and create ASN.1 algorithm identifiers such as those used in PKCS #7 and other protocols. You call B\_SetAlgorithmInfo to initialize an algorithm object from the encoded algorithm identifier that includes the hash function, mask generator function, and P source function. You call B\_GetAlgorithmInfo with this AI to create an encoded algorithm identifier from an algorithm object that was created using AI\_PKCS\_OAEPRecode or AI\_PKCS\_OAEPRecodeBER. The OID for the RSA OAEP encryption, excluding the tag and length bytes, in decimal, is "42, 134, 72, 134, 247, 13, 1, 1, 7". The OID for the mask function, excluding the tag and length bytes, in decimal, is "42, 134, 72, 134, 247, 13, 1, 1, 8". The OID for the P source function, excluding the tag and length bytes, in decimal, is "42, 134, 72, 134, 247, 13, 1, 1, 9". Also see AI\_PKCS\_OAEPRecode.

### Type of information this allows you to use:

OAEP message padding as defined in PKCS #1 v2.0 (DRAFT 1- July 14, 1998). When encoding, this algorithm encodes the data according to the definition of EME-OAEP-Encode as specified in PKCS #1 v2.0. When decoding, this algorithm decodes the data according to the definition of EME-OAEP-Decode.

This permits the use of raw or hardware-based RSA with the PKCS #1 v2.0 flavor of Optimal Asymmetric Encryption Padding.

### Format of info supplied to B\_SetAlgorithmInfo:

pointer to an ITEM structure that gives the address and length of the BER-encoded algorithm identifier. The encoding is converted to DER before it is copied to the algorithm object. B\_SetAlgorithmInfo returns BE\_WRONG\_ALGORITHM\_INFO if the algorithm identifier specifies an algorithm other than RSAES-OAEP Encryption as specified by PKCS #1 v2.0.

The general ASN.1 syntax for RSAES-OAEP is complicated, the simple DER encoding

of the default algorithm is given first, followed by the general syntax.

```
-- Default Algorithm Identifier for RSAES-OAEP.
-- The DER Encoding of this is in hexadecimal given below.
-- Notice that the DER encoding of the default parameters
-- is just an empty sequence.
-- 30 0D
--   06 09
--     2A 86 48 86 F7 0D 01 01 07
--   30 00
--
RSAES-OAEP-Default-Identifier ::= AlgorithmIdentifier {
  id-RSAES-OAEP,
  { sha1Identifier,
    mgf1SHA1Identifier,
    pSpecifiedEmptyIdentifier
  }
}
```

The general syntax is:

```
RSAES-OAEP ::= Sequence {
  algorithm OBJECT IDENTIFIER (id-RSAES-OAEP),
  parameters RSAES-OAEP-params
}
-- Identifier for PKCS #1 v2.0 OAEP.
-- The DER for this in hexadecimal is:
-- 06 09
--   2A 86 48 86 F7 0D 01 01 07
--
id-RSAES-OAEP OBJECT IDENTIFIER ::= {
  iso(1) member-body(2) us(840) rsadsi (113549)
  pkcs(1) pkcs-1(1) RSAES-OAEP(7)}
-- Identifier for the PKCS #1 v2.0 mask generation function,
-- which takes a hash function AlgID as a parameter.
-- The DER for this in hexadecimal is:
-- 06 09
--   2A 86 48 86 F7 0D 01 01 08
--
id-mgf1 OBJECT IDENTIFIER ::= {
  iso(1) member-body(2) us(840) rsadsi (113549)
  pkcs(1) pkcs-1(1) mgf1(8)}
```

```

-- The identifier says that the algorithm by which the P
-- string for RSAES-OAEP is generated is by setting it
-- equal to the contents of the OCTET STRING which is
-- the parameter for this AlgorithmIdentifier.
-- The DER for this in hexadecimal is:
-- 06 09
-- 2A 86 48 86 F7 0D 01 01 09
--
id-pSpecified OBJECT IDENTIFIER ::= {
    iso(1) member-body(2) us(840) rsadsi(113549)
    pkcs(1) pkcs-1(1) pSpecified(9)}
-- Identifier for the SHA1 digest function.
-- The DER for this in hexadecimal is:
-- 06 05
-- 2B 0E 03 02 1A
--
id-sha1 OBJECT IDENTIFIER ::= {
    iso(1) identified-organization(3) oiw(14) secsig(3)
    algorithms(2) sha1(26) }
-- Syntax of AlgorithmIdentifier.parameters for RSAES-OAEP.
-- Note that the tags in this Sequence are explicit.
-- The DER encoding of DEFAULT values is to omit them.
--
RSAES-OAEP-params ::= SEQUENCE {
    hashFunc      [0] AlgorithmIdentifier {
        {oaepDigestAlgorithms} }
        DEFAULT sha1Identifier,
    maskGenFunc   [1] AlgorithmIdentifier {
        {pkcs1MGFAlgorithms} }
        DEFAULT mgf1SHA1Identifier,
    pSourceFunc   [2] AlgorithmIdentifier {
        {pkcs1PGenAlgorithms} }
        DEFAULT pSpecifiedEmptyIdentifier
}
-- Algorithm Identifier for SHA1, which is the OAEP default.
--
sha1Identifier ::= AlgorithmIdentifier {
    id-sha1, NULL }
-- Default AlgorithmIdentifier for id-RSAES-OAEP.maskGenFunc.
--

```

```

mgf1SHA1Identifier ::= AlgorithmIdentifier {
    id-mgf1, sha1Identifier }
-- This identifier means that P is an empty string, so the digest
-- of the empty string appears in the RSA block before masking.
--
pSpecifiedEmptyIdentifier ::= AlgorithmIdentifier {
    id-pSpecified, OCTET STRING SIZE (0)
}

```

## Format of info supplied to B\_GetAlgorithmInfo:

pointer to an ITEM structure that gives the address and length of the DER-encoded algorithm identifier.

## Crypto-C procedures to use with algorithm object:

B\_EncodeInit, B\_EncodeUpdate, B\_EncodeFinal, B\_DecodeInit, B\_DecodeUpdate, and B\_DecodeFinal.

The final call to B\_EncodeUpdate does not contain message data. Rather, the trailing call to B\_EncodeUpdate is included to pass in a number of random seed bytes for the OAEP encoding process. It is recommended that the caller use AI\_X962Random\_V0 or AI\_SHA1Random to generate hLen bytes initialized with 160 bits of entropy. The default digest algorithm for PKCS #1 v2.0 OAEP is SHA1. SHA1 produces a digest of 20 bytes, so hLen for SHA1 is 20 bytes.

B\_Decode\_Update does not contain an extra call for seed bytes.

## Algorithm methods to include in application's algorithm chooser:

AM\_SHA is required for the default *pSource* digest function and also for the default MGF underlying digest method.

## Compatible representation:

AI\_PKCS\_OAEPRecodeBER.

## Input constraints:

The total number of bytes to encode must be at least  $[(2 * hLen) + 1]$  bytes long.

## Output considerations:

The output of encoding will be an encoded message that is the same size as *maxPartOutLen*. (See `B_EncodeUpdate`, `B_EncodeFinal`, `B_DecodeUpdate`, and `B_DecodeFinal`.) The output of the decoding will be the original message.

## AI\_PKCS\_RSAPrivate

### Purpose:

This AI allows you to decrypt data encrypted using the RSA public-key cryptosystem as defined in PKCS #1.

### Type of information this allows you to use:

the RSA algorithm for performing private key decryption as defined in PKCS #1. When encrypting, this algorithm encodes the data according to block type 01. When decrypting, this algorithm decodes the data from a block type 02.

### Format of *info* supplied to B\_SetAlgorithmInfo:

NULL\_PTR.

### Format of *info* returned by B\_GetAlgorithmInfo:

NULL\_PTR.

### Crypto-C procedures to use with algorithm object:

B\_EncryptInit, B\_EncryptUpdate, B\_EncryptFinal, B\_DecryptInit, B\_DecryptUpdate, and B\_DecryptFinal. You may pass (B\_ALGORITHM\_OBJ) NULL\_PTR for all *randomAlgorithm* arguments.

### Algorithm methods to include in application's algorithm chooser:

AM\_RSA\_CRT\_ENCRYPT or AM\_RSA\_CRT\_ENCRYPT\_BLI ND for encryption, or AM\_RSA\_CRT\_DECRYPT or AM\_RSA\_CRT\_DECRYPT\_BLI ND for decryption.

AM\_RSA\_CRT\_ENCRYPT\_BLI ND and AM\_RSA\_CRT\_DECRYPT\_BLI ND perform blinding to protect against timing attacks, whereas AM\_RSA\_CRT\_ENCRYPT and AM\_RSA\_CRT\_DECRYPT do not.

### Key info types for *keyObject* in B\_EncryptInit or B\_DecryptInit:

KI\_RSA\_CRT, KI\_PKCS\_RSAPrivate, KI\_PKCS\_RSAPrivateBER, or KI\_RSAPrivateBSAFE1.

## Compatible representation:

AI\_PKCS\_RSAPrivateBER, AI\_PKCS\_RSAPrivatePEM.

## Input constraints:

The total number of bytes to encrypt may not be more than  $k - 11$ , where  $k$  is the key's modulus size in bytes.

## Output considerations:

The output of encryption will be the same size as the key's modulus.

## AI\_PKCS\_RSAPrivateBER

### Purpose:

This AI is similar to AI\_PKCS\_RSAPrivate except that it uses the ASN.1 BER format. This AI allows you to parse and create ASN.1 algorithm identifiers such as those used in PKCS #7 and other protocols. You call B\_SetAlgorithmInfo to initialize an algorithm object from the encoded algorithm identifier. You call B\_GetAlgorithmInfo with this AI to create an encoded algorithm identifier from an algorithm object that was created using AI\_PKCS\_RSAPrivate, AI\_PKCS\_RSAPrivateBER or AI\_PKCS\_RSAPrivatePEM. The OID for this algorithm, excluding the tag and length bytes, in decimal is "42, 134, 72, 134, 247, 13, 1, 1, 1"

### Type of information this allows you to use:

the encoding of an algorithm identifier that specifies the RSA algorithm for performing private key decryption as defined in PKCS #1. When encrypting, this algorithm encodes the data according to block type 01. When decrypting, this algorithm decodes the data from a block type 02.

### Format of *info* supplied to B\_SetAlgorithmInfo:

pointer to an ITEM structure that gives the address and length of the BER-encoded algorithm identifier. The encoding is converted to DER before it is copied to the algorithm object. B\_SetAlgorithmInfo returns BE\_WRONG\_ALGORITHM\_INFO if the algorithm identifier specifies an algorithm other than RSA Encryption.

### Format of *info* returned by B\_GetAlgorithmInfo:

pointer to an ITEM structure that gives the address and length of the DER-encoded algorithm identifier.

### Crypto-C procedures to use with algorithm object:

B\_EncryptInit, B\_EncryptUpdate, B\_EncryptFinal, B\_DecryptInit, B\_DecryptUpdate, and B\_DecryptFinal. You may pass (B\_ALGORITHM\_OBJ)NULL\_PTR for all *randomAlgorithm* arguments.

### Algorithm methods to include in application's algorithm chooser:

AM\_RSA\_CRT\_ENCRYPT or AM\_RSA\_CRT\_ENCRYPT\_BLIND for encryption, or

AM\_RSA\_CRT\_DECRYPT or AM\_RSA\_CRT\_DECRYPT\_BLI ND for decryption.

AM\_RSA\_CRT\_ENCRYPT\_BLI ND and AM\_RSA\_CRT\_DECRYPT\_BLI ND perform blinding to protect against timing attacks, whereas AM\_RSA\_CRT\_ENCRYPT and AM\_RSA\_CRT\_DECRYPT do not.

### **Key info types for *keyObject* in B\_EncryptInit or B\_DecryptInit:**

KI\_RSA\_CRT, KI\_PKCS\_RSAPri vate, KI\_PKCS\_RSAPri vateBER, or KI\_RSAPri vateBSAFE1.

### **Compatible representation:**

AI\_PKCS\_RSAPri vate, AI\_PKCS\_RSAPri vatePEM.

### **Input constraints:**

The total number of bytes to encrypt may not be more than  $k - 11$ , where  $k$  is the key's modulus size in bytes.

### **Output considerations:**

The output of encryption will be the same size as the key's modulus.

## AI\_PKCS\_RSAPrivatePEM

### Purpose:

This AI is similar to AI\_PKCS\_RSAPrivate except that it uses the PEM format. This AI allows you to parse and create PEM algorithm identifiers such as those used in Privacy Enhanced Mail protocol. You call B\_SetAlgorithmInfo to initialize an algorithm object from the encoded algorithm identifier. You call B\_GetAlgorithmInfo with this AI to create an encoded algorithm identifier from an algorithm object that was created using AI\_PKCS\_RSAPrivate, AI\_PKCS\_RSAPrivateBER or AI\_PKCS\_RSAPrivatePEM.

### Type of information this allows you to use:

an RFC 1423 identifier that specifies the RSA algorithm for performing private key decryption as defined in PKCS #1. When encrypting, this algorithm encodes the data according to block type 01. When decrypting, this algorithm decodes the data from a block type 02.

This algorithm info type is intended to process the asymmetric encryption identifier in a MIC-Info and Key-Info field in a PEM encapsulated header.

### Format of *info* supplied to B\_SetAlgorithmInfo:

pointer to a null-terminated string (char \*) that gives the RSA identifier, for example, "RSA". Space and tab characters are removed from the string before it is copied to the algorithm object. B\_SetAlgorithmInfo returns BE\_WRONG\_ALGORITHM\_INFO if the algorithm identifier specifies an identifier other than RSA.

### Format of *info* returned by B\_GetAlgorithmInfo:

pointer to a null-terminated string that gives the RSA identifier.

### Crypto-C procedures to use with algorithm object:

B\_EncryptInit, B\_EncryptUpdate, B\_EncryptFinal, B\_DecryptInit, B\_DecryptUpdate, and B\_DecryptFinal. You may pass (B\_ALGORITHM\_OBJ)NULL\_PTR for all *randomAlgorithm* arguments.

## Algorithm methods to include in application's algorithm chooser:

AM\_RSA\_CRT\_ENCRYPT or AM\_RSA\_CRT\_ENCRYPT\_BLI ND for encryption, or AM\_RSA\_CRT\_DECRYPT or AM\_RSA\_CRT\_DECRYPT\_BLI ND for decryption. AM\_RSA\_CRT\_ENCRYPT\_BLI ND and AM\_RSA\_CRT\_DECRYPT\_BLI ND perform blinding to protect against timing attacks, whereas AM\_RSA\_CRT\_ENCRYPT and AM\_RSA\_CRT\_DECRYPT do not.

## Key info types for *keyObject* in B\_EncryptInit or B\_DecryptInit:

KI\_RSA\_CRT, KI\_PKCS\_RSAPri vate, KI\_PKCS\_RSAPri vateBER or KI\_RSAPri vateBSAFE1.

## Compatible representation:

AI\_PKCS\_RSAPri vate, AI\_PKCS\_RSAPri vateBER.

## Input constraints:

The total number of bytes to encrypt may not be more than  $k - 11$ , where  $k$  is the keys modulus size in bytes.

## Output considerations:

The output of encryption will be the same size as the key's modulus.

## AI\_PKCS\_RSAPublic

### Purpose:

This AI allows you to encrypt data using the RSA public-key cryptosystem as defined in PKCS #1.

### Type of information this allows you to use:

the RSA algorithm for performing public key encryption as defined in PKCS #1. When encrypting, this algorithm encodes the data according to block type 02. When decrypting, this algorithm decodes the data from block type 01.

### Format of *info* supplied to B\_SetAlgorithmInfo:

NULL\_PTR.

### Format of *info* returned by B\_GetAlgorithmInfo:

NULL\_PTR.

### Crypto-C procedures to use with algorithm object:

B\_EncryptInit, B\_EncryptUpdate, B\_EncryptFinal, and B\_DecryptInit, B\_DecryptUpdate, and B\_DecryptFinal. Note that B\_EncryptUpdate and B\_EncryptFinal require a random algorithm. You may pass (B\_ALGORITHM\_OBJ) NULL\_PTR for the *randomAlgorithm* argument in B\_DecryptUpdate and B\_DecryptFinal.

### Algorithm methods to include in application's algorithm chooser:

AM\_RSA\_ENCRYPT for encryption or AM\_RSA\_DECRYPT for decryption.

### Key info types for *keyObject* in B\_EncryptInit or B\_DecryptInit:

KI\_RSAPublic, KI\_RSAPublicBER, or KI\_RSAPublicSAFE1.

### Compatible representation:

AI\_PKCS\_RSAPublicBER, AI\_PKCS\_RSAPublicPEM.

### **Input constraints:**

The total number of bytes to encrypt may not be more than  $k - 11$ , where  $k$  is the key's modulus size in bytes.

### **Output considerations:**

The output of encryption will be the same size as the key's modulus.

## AI\_PKCS\_RSAPublicBER

### Purpose:

This AI is similar to AI\_PKCS\_RSAPublic except that it uses the ASN.1 BER format. This AI allows you to parse and create ASN.1 algorithm identifiers such as those used in PKCS #7 and other protocols. You call B\_SetAlgorithmInfo to initialize an algorithm object from the encoded algorithm identifier. You call B\_GetAlgorithmInfo with this AI to create an encoded algorithm identifier from an algorithm object that was created using AI\_PKCS\_RSAPublic, AI\_PKCS\_RSAPublicBER or AI\_PKCS\_RSAPublicPEM. The OID for this algorithm, excluding the tag and length bytes, in decimal is "42, 134, 72, 134, 247, 13, 1, 1, 1".

### Type of information this allows you to use:

the encoding of an algorithm identifier that specifies the RSA algorithm for performing public key encryption as defined in PKCS #1. When encrypting, this algorithm encodes the data according to block type 02. When decrypting, this algorithm decodes the data from block type 01.

### Format of *info* supplied to B\_SetAlgorithmInfo:

pointer to an ITEM structure that gives the address and length of the BER-encoded algorithm identifier. The encoding is converted to DER before it is copied to the algorithm object. B\_SetAlgorithmInfo returns BE\_WRONG\_ALGORITHM\_INFO if the algorithm identifier specifies an algorithm other than RSA Encryption.

### Format of *info* returned by B\_GetAlgorithmInfo:

pointer to an ITEM structure that gives the address and length of the DER-encoded algorithm identifier.

### Crypto-C procedures to use with algorithm object:

B\_EncryptInit, B\_EncryptUpdate, B\_EncryptFinal, B\_DecryptInit, B\_DecryptUpdate, and B\_DecryptFinal. Note that B\_EncryptUpdate and B\_EncryptFinal require a random algorithm. You may pass (B\_ALGORITHM\_OBJ)NULL\_PTR for the *randomAlgorithm* argument in B\_DecryptUpdate and B\_DecryptFinal.

## Algorithm methods to include in application's algorithm chooser:

AM\_RSA\_ENCRYPT for encryption and AM\_RSA\_DECRYPT for decryption.

## Key info types for *keyObject* in B\_EncryptInit or B\_DecryptInit:

KI\_RSAPublic, KI\_RSAPublicBER or KI\_RSAPublicBSAFE1.

## Compatible representation:

AI\_PKCS\_RSAPublic, AI\_PKCS\_RSAPublicPEM.

## Input constraints:

The total number of bytes to encrypt may not be more than  $k - 11$ , where  $k$  is the key's modulus size in bytes.

## Output considerations:

The output of encryption will be the same size as the key's modulus.

## AI\_PKCS\_RSAPublicPEM

### Purpose:

This AI is similar to AI\_PKCS\_RSAPublic except that it uses the PEM format. This AI allows you to parse and create PEM algorithm identifiers such as used in Privacy Enhanced Mail protocol. You call B\_SetAlgorithmInfo to initialize an algorithm object from the encoded algorithm identifier. You call B\_GetAlgorithmInfo with this AI to create an encoded algorithm identifier from an algorithm object that was created using AI\_PKCS\_RSAPublic, AI\_PKCS\_RSAPublicBER, or AI\_PKCS\_RSAPublicPEM.

### Type of information this allows you to use:

an RFC 1423 identifier that specifies the RSA algorithm for performing public key encryption as defined in PKCS #1. When encrypting, this algorithm encodes the data according to block type 02. When decrypting, this algorithm decodes the data from a block type 01. This algorithm info type is intended to process the asymmetric encryption identifier in a MIC-Info and Key-Info field in a PEM encapsulated header.

### Format of *info* supplied to B\_SetAlgorithmInfo:

pointer to a null-terminated string (char \*) that gives the RSA identifier. For example, "RSA". Space and tab characters are removed from the string before it is copied to the algorithm object. B\_SetAlgorithmInfo returns BE\_WRONG\_ALGORITHM\_INFO if the algorithm identifier specifies an identifier other than RSA.

### Format of *info* returned by B\_GetAlgorithmInfo:

pointer to a null-terminated string that gives the RSA identifier.

### Crypto-C procedures to use with algorithm object:

B\_EncryptInit, B\_EncryptUpdate, B\_EncryptFinal, B\_DecryptInit, B\_DecryptUpdate, and B\_DecryptFinal. Note that B\_EncryptUpdate and B\_EncryptFinal require a random algorithm. You may pass (B\_ALGORITHM\_OBJ)NULL\_PTR for the *randomAlgorithm* argument in B\_DecryptUpdate and B\_DecryptFinal.

### Algorithm methods to include in application's algorithm chooser:

AM\_RSA\_ENCRYPT for encryption or AM\_RSA\_DECRYPT for decryption.

## Key info types for *keyObject* in B\_EncryptInit or B\_DecryptInit:

KI\_RSAPublic, KI\_RSAPublicBER, or KI\_RSAPublicBSAFE1.

## Compatible representation:

AI\_PKCS\_RSAPublic, AI\_PKCS\_RSAPublicBER.

## Input constraints:

The total number of bytes to encrypt may not be more than  $k - 11$ , where  $k$  is the key's modulus size in bytes.

## Output considerations:

The output of encryption will be the same size as the key's modulus.

## AI\_RC2\_CBC

### Purpose:

This AI allows you to perform RC2 encryption or decryption in CBC mode with an 8-byte initialization vector. During encryption, this algorithm does not pad the output. Thus, you must provide input that is a multiple of 8 bytes. See AI\_RC2\_CBCPad for the same algorithm with padding. RC2 is a variable-key-size block cipher which means that the key can be anywhere between 1 and 128 bytes. The larger the key, the greater the security. RC2 is described in RFC 2268, and the CBC mode is similar to the one described in RFC 2040.

Other algorithms that can be used for encryption/decryption in CBC mode without padding are AI\_DES\_CBC\_IV8, AI\_DES\_EDE3\_CBC\_IV8, AI\_DESX\_CBC\_IV8, and AI\_RC5\_CBC.

### Type of information this allows you to use:

an effective key size and an 8-byte initialization vector for the RC2-CBC encryption algorithm.

### Format of *info* supplied to B\_SetAlgorithmInfo:

pointer to an A\_RC2\_CBC\_PARAMS structure:

```
typedef struct {
    unsigned int    effectiveKeyBits;           /* effective key size in bits */
    unsigned char  *iv;                         /* initialization vector */
} A_RC2_CBC_PARAMS;
```

### Format of *info* returned by B\_GetAlgorithmInfo:

pointer to an A\_RC2\_CBC\_PARAMS structure (see above).

### Crypto-C procedures to use with algorithm object:

B\_EncryptInit, B\_EncryptUpdate, B\_EncryptFinal, B\_DecryptInit, B\_DecryptUpdate, and B\_DecryptFinal. You may pass (B\_ALGORITHM\_OBJ) NULL\_PTR for all *randomAlgorithm* arguments.

## Algorithm methods to include in application's algorithm chooser:

AM\_RC2\_CBC\_ENCRYPT for encryption and AM\_RC2\_CBC\_DECRYPT for decryption.

## Key info types for *keyObject* in B\_EncryptInit or B\_DecryptInit:

KI\_8Byte, KI\_Item, KI\_RC2WithBSAFE1Params, or KI\_RC2\_BSAFE1.

## Input constraints:

During encryption, this algorithm does not pad the output. Thus, you must provide input that is a multiple of 8 bytes.

## Token-based algorithm methods:



AI\_RC2\_CBC may be used to access the hardware-related algorithm methods AM\_TOKEN\_RC2\_CBC\_ENCRYPT and AM\_TOKEN\_RC2\_CBC\_DECRYPT, for use with BHAPI.

## Token-based key info types:

When used with one of the hardware algorithm methods listed above, AI\_RC2\_CBC should be used with KI\_Token or KI\_ExtendedToken.

## AI\_RC2\_CBC\_BSAFE1

### Purpose:

Deprecated. This AI is included only for backward compatibility.

### Type of information this allows you to use:

the encryption type parameter (pad, pad with checksum, or raw) for the RC2 encryption algorithm as defined by BSAFE 1.x. Note that RC2 is the same as SX1.

### Format of *info* supplied to `B_SetAlgorithmInfo`:

pointer to a `B_BSAFE1_ENCRYPTI ON_PARAMS` structure:

```
typedef struct {
    int encrypti onType;           /* encrypti on type */
} B_BSAFE1_ENCRYPTI ON_PARAMS;
```

*encrypti onType* should be set to `B_BSAFE1_PAD` for pad mode, `B_BSAFE1_PAD_CHECKSUM` for pad with checksum mode, or `B_BSAFE1_RAW` for raw mode.

### Format of *info* returned by `B_GetAlgorithmInfo`:

pointer to a `B_BSAFE1_ENCRYPTI ON_PARAMS` structure (see above).

### Crypto-C procedures to use with algorithm object:

`B_EncryptI nit`, `B_EncryptUpdate`, `B_EncryptFi nal`, `B_DecryptI nit`, `B_DecryptUpdate`, and `B_DecryptFi nal`. You may pass `(B_ALGORI THM_OB J) NULL_PTR` for all *randomAl gori thm* arguments.

### Algorithm methods to include in application's algorithm chooser:

`AM_RC2_CBC_ENCRYPT` for encryption and `AM_RC2_CBC_DECRYPT` for decryption.

### Key info types for *keyObject* in `B_EncryptI nit` or `B_DecryptI nit`:

`KI_RC2Wi thBSAFE1Params` or `KI_RC2_BSAFE1`.

## **Input constraints:**

During encryption, this algorithm does not pad the output. Thus, you must provide input that is a multiple of 8 bytes.

## **Output considerations:**

In pad mode, the total number of output bytes from encryption can be as many as 8 more than the total input. In pad with checksum mode, the total number of output bytes from encryption can be as many as 16 more than the total input.

## AI\_RC2\_CBCPad

### Purpose:

This AI allows you to perform RC2 encryption or decryption in CBC mode with an 8-byte initialization vector. This algorithm pads as described in PKCS #5, so the input data does not have to be a multiple of 8 bytes. RC2 is a variable-key-size block cipher which means that the key can be anywhere between 1 and 128 bytes. The larger the key, the greater the security. RC2 is described in RFC 2268, and CBC mode is similar to the one described in RFC 2040.

Other algorithms that can be used for encryption/decryption in CBC mode with padding are AI\_DES\_CBCPadI V8, AI\_DES\_EDE3\_CBCPadI V8, AI\_DESX\_CBCPadI V8, and AI\_RC5\_CBCPad.

### Type of information this allows you to use:

an 8-byte initialization vector and effective key size for the RC2-CBC With Padding encryption algorithm.

### Format of *info* supplied to B\_SetAlgorithmInfo:

pointer to an A\_RC2\_CBC\_PARAMS structure:

```
typedef struct {
    unsigned int    effectiveKeyBits;           /* effective key size in bits */
    unsigned char  *iv;                         * initialization vector */
} A_RC2_CBC_PARAMS;
```

### Format of *info* returned by B\_GetAlgorithmInfo:

pointer to an A\_RC2\_CBC\_PARAMS structure (see above).

### Crypto-C procedures to use with algorithm object:

B\_EncryptInit, B\_EncryptUpdate, B\_EncryptFinal, B\_DecryptInit, B\_DecryptUpdate, and B\_DecryptFinal. You may pass (B\_ALGORITHM\_OBJ) NULL\_PTR for all *randomAlgorithm* arguments.

### **Algorithm methods to include in application's algorithm chooser:**

AM\_RC2\_CBC\_ENCRYPT for encryption and AM\_RC2\_CBC\_DECRYPT for decryption.

### **Key info types for *keyObject* in B\_EncryptInit or B\_DecryptInit:**

KI\_8Byte, KI\_Item, KI\_RC2WithBSAFE1Params, or KI\_RC2\_BSAFE1.

### **Compatible representation:**

AI\_RC2\_CBCPadBER, AI\_RC2\_CBCPadPEM.

### **Output considerations:**

During encryption, this AI pads the output. Thus, the total number of output bytes from encryption can be as many as 8 bytes more than the total output.

## AI\_RC2\_CBCPadBER

### Purpose:

This AI is similar to AI\_RC2\_CBCPad except that it uses the ASN.1 BER format. This AI allows you to parse and create ASN.1 algorithm identifiers such as used in PKCS #7 and other protocols. You call `B_SetAlgorithmInfo` to initialize an algorithm object from the encoded algorithm identifier which includes ASN.1 encoding of the `A_RC2_CBC_PARAMS` structure defined in the description of AI\_RC2\_CBCPad. You call `B_GetAlgorithmInfo` with this AI to create an encoded algorithm identifier from an algorithm object that was created using AI\_RC2\_CBCPad, AI\_RC2\_CBCPadBER or AI\_RC2\_CBCPadPEM. The OID for this algorithm, excluding the tag and length bytes, in decimal is "42, 134, 72, 134, 247, 13, 3, 2".

### Type of information this allows you to use:

the encoding of an algorithm identifier that specifies the RC2-CBC With Padding encryption algorithm.

### Format of *info* supplied to `B_SetAlgorithmInfo`:

pointer to an `ITEM` structure that gives the address and length of the BER-encoded algorithm identifier. The encoding is converted to DER before it is copied to the algorithm object. `B_SetAlgorithmInfo` returns `BE_WRONG_ALGORITHM_INFO` if the algorithm identifier specifies an algorithm other than RC2-CBC With Padding.

### Format of *info* returned by `B_GetAlgorithmInfo`:

pointer to an `ITEM` structure that gives the address and length of the DER-encoded algorithm identifier.

### Crypto-C procedures to use with algorithm object:

`B_EncryptInit`, `B_EncryptUpdate`, `B_EncryptFinal`, `B_DecryptInit`, `B_DecryptUpdate`, and `B_DecryptFinal`. You may pass `(B_ALGORITHM_OBJ)NULL_PTR` for all *randomAlgorithm* arguments.

### Algorithm methods to include in application's algorithm chooser:

`AM_RC2_CBC_ENCRYPT` for encryption and `AM_RC2_CBC_DECRYPT` for decryption.

## Key info types for *keyObject* in B\_EncryptInit or B\_DecryptInit:

KI\_8Byte, KI\_Item, KI\_RC2WithBSAFE1Params, or KI\_RC2\_BSAFE1.

## Compatible representation:

AI\_RC2\_CBCPad, AI\_RC2\_CBCPadPEM.

## Output considerations:

During encryption, this AI pads the output. Thus, the total number of output bytes from encryption can be as many as 8 bytes more than the total output.

## AI\_RC2\_CBCPadPEM

### Purpose:

This AI is similar to AI\_RC2\_CBCPad except that it uses the PEM format. This AI allows you to parse and create PEM algorithm identifiers such as used in Privacy Enhanced Mail protocol. You call `B_SetAlgorithmInfo` to initialize an algorithm object from the encoded algorithm identifier which includes PEM encoding of the `A_RC2_CBC_PARAMS` structure defined in the description of AI\_RC2\_CBCPad. You call `B_GetAlgorithmInfo` with this AI to create an encoded algorithm identifier from an algorithm object that was created using AI\_RC2\_CBCPad, AI\_RC2\_CBCPadBER, or AI\_RC2\_CBCPadPEM.

### Type of information this allows you to use:

an RFC 1423-style identifier that specifies the RC2-CBC With Padding encryption algorithm. This algorithm info type is intended to process the value of a DEK-Info field in a PEM encapsulated header.

### Format of *info* supplied to `B_SetAlgorithmInfo`:

pointer to a null-terminated string (char \*) that gives the RC2-CBC identifier and parameters. For example, "RC2-CBC, BAgrIj NEVWZ3i A==". Space and tab characters are removed from the string before it is copied to the algorithm object.

`B_SetAlgorithmInfo` returns `BE_WRONG_ALGORITHM_INFO` if the algorithm identifier specifies an identifier other than RC2-CBC.

### Format of *info* returned by `B_GetAlgorithmInfo`:

pointer to a null-terminated string that gives the RC2-CBC identifier and parameters.

### Crypto-C procedures to use with algorithm object:

`B_EncryptInit`, `B_EncryptUpdate`, `B_EncryptFinal`, `B_DecryptInit`, `B_DecryptUpdate`, and `B_DecryptFinal`. You may pass `(B_ALGORITHM_OBJ)NULL_PTR` for all *randomAlgorithm* arguments.

### Algorithm methods to include in application's algorithm chooser:

`AM_RC2_CBC_ENCRYPT` for encryption and `AM_RC2_CBC_DECRYPT` for decryption.

### **Key info types for *keyObject* in B\_EncryptInit or B\_DecryptInit:**

KI\_8Byte, KI\_Item, KI\_RC2WithBSAFE1Params, or KI\_RC2\_BSAFE1.

### **Compatible representation:**

AI\_RC2\_CBCPad, AI\_RC2\_CBCPadBER.

### **Output considerations:**

During encryption, this AI pads the output. Thus, the total number of output bytes from encryption can be as many as 8 bytes more than the total output.

---

## AI\_RC4

### Purpose:

This AI allows you to perform RC4 encryption and decryption. RC4 is a stream cipher and its description can be found in B. Schneier's book *Applied Cryptography*. Because it is a stream cipher, there are no restrictions on the length of input data. A similar algorithm that allows you to authenticate the encrypted data is AI\_RC4WithMAC.

### Type of information this allows you to use:

the RC4 encryption algorithm.

### Format of *info* supplied to B\_SetAlgorithmInfo:

NULL\_PTR.

### Format of *info* returned by B\_GetAlgorithmInfo:

NULL\_PTR.

### Crypto-C procedures to use with algorithm object:

B\_EncryptInit, B\_EncryptUpdate, B\_EncryptFinal, B\_DecryptInit, B\_DecryptUpdate, and B\_DecryptFinal. You may pass (B\_ALGORITHM\_OBJ)NULL\_PTR for all *randomAlgorithm* arguments.

Due to the nature of the RC4 algorithm, security is compromised if multiple data blocks are encrypted with the same RC4 key. Therefore, B\_EncryptUpdate cannot be called after B\_EncryptFinal. To begin an encryption operation for a new data block, you must call B\_EncryptInit and supply a new key.

### Algorithm methods to include in application's algorithm chooser:

AM\_RC4\_ENCRYPT for encryption and AM\_RC4\_DECRYPT for decryption.

### Key info types for *keyObject* in B\_EncryptInit or B\_DecryptInit:

KI\_Item that gives the address and length of the RC4 key.

## Compatible representation:

AI\_RC4\_BER.

## Token-based algorithm methods:



AI\_RC4 may be used to access the hardware-related algorithm methods AM\_TOKEN\_RC4\_ENCRYPT and AM\_TOKEN\_RC4\_DECRYPT, for use with BHAPI.

## Token-based key info types:

When used with one of the hardware algorithm methods listed above, AI\_RC4 should be used with KI-Token or KI\_ExtendedToken.

## AI\_RC4\_BER

### Purpose:

This AI is similar to AI\_RC4 except that it uses the ASN.1 BER format. This AI allows you to parse and create ASN.1 algorithm identifiers such as those used in PKCS #7 and other protocols. You call `B_SetAlgorithmInfo` to initialize an algorithm object from the encoded algorithm identifier. You call `B_GetAlgorithmInfo` with this AI to create an encoded algorithm identifier from an algorithm object that was created using AI\_RC4 or AI\_RC4\_BER. The OID for this algorithm, excluding the tag and length bytes, in decimal is "42, 134, 72, 134, 247, 13, 3, 4".

### Type of information this allows you to use:

the encoding of an algorithm identifier that specifies the RC4 encryption algorithm.

### Format of *info* supplied to `B_SetAlgorithmInfo`:

pointer to an ITEM structure that gives the address and length of the BER-encoded algorithm identifier. The encoding is converted to DER before it is copied to the algorithm object. `B_SetAlgorithmInfo` returns `BE_WRONG_ALGORITHM_INFO` if the algorithm identifier specifies an algorithm other than RC4.

### Format of *info* returned by `B_GetAlgorithmInfo`:

pointer to an ITEM structure that gives the address and length of the DER-encoded algorithm identifier.

### Crypto-C procedures to use with algorithm object:

`B_EncryptInit`, `B_EncryptUpdate`, `B_EncryptFinal`, `B_DecryptInit`, `B_DecryptUpdate`, and `B_DecryptFinal`. You may pass `(B_ALGORITHM_OBJ)NULL_PTR` for all *randomAlgorithm* arguments.

Due to the nature of the RC4 algorithm, security is compromised if multiple data blocks are encrypted with the same RC4 key. Therefore, `B_EncryptUpdate` cannot be called after `B_EncryptFinal`. To begin an encryption operation for a new data block, you must call `B_EncryptInit` and supply a new key.

**Algorithm methods to include in application's algorithm chooser:**

AM\_RC4\_ENCRYPT for encryption and AM\_RC4\_DECRYPT for decryption.

**Key info types for *keyObject* in B\_EncryptInit or B\_DecryptInit:**

KI\_Item that gives the address and length of the RC4 key.

**Compatible representation:**

AI\_RC4.

## AI\_RC4WithMAC

### Purpose:

This AI implements a stream cipher with a simple tamper-detection message authentication code based on AI\_MAC. When applied to a plaintext buffer of N bytes, it produces a ciphertext of N bytes using the same algorithm as AI\_RC4, and then it appends a MAC of macLen bytes. You can find the description of AI\_RC4 in B. Schneier's *Applied Cryptography*, and the detailed description of AI\_MAC can be found in Appendix B.

### Type of information this allows you to use:

the RC4 With MAC encryption algorithm. The MAC is computed using AI\_MAC by first passing the key to AI\_MAC, then the plaintext, and finally a block of macLen zero bytes. The resulting value from AI\_MAC is appended to the ciphertext. For decryption, the MAC value is checked.

The key passed to both AI\_RC4 and AI\_MAC is created by appending the salt bytes to the end of the key passed to B\_EncryptI ni t or B\_DecryptI ni t. That is, for this AI, the RC4 key depends on the salt as well as the key object passed to I ni t routine.

### Format of *info* supplied to B\_SetAlgorithmInfo:

pointer to a B\_RC4\_WI TH\_MAC\_PARAMS structure:

```
typedef struct {
    I TEM          sal t;                /* variable-length sal t */
    unsigned int  macLen;              /* length to use for MAC value */
} B_RC4_WI TH_MAC_PARAMS;
```

The *sal t* I TEM supplies the salt value that is appended to the key, where the I TEM's *data* points to an unsigned byte array and the I TEM's *len* gives its length. If the length is zero, no salt is appended to the key, and the I TEM's *data* is ignored. *macLen* has a minimum of 2 and maximum of 16.

### Format of *info* returned by B\_GetAlgorithmInfo:

pointer to a B\_RC4\_WI TH\_MAC\_PARAMS structure (see above).

## Crypto-C procedures to use with algorithm object:

`B_EncryptInit`, `B_EncryptUpdate`, `B_EncryptFinal`, `B_DecryptInit`, `B_DecryptUpdate`, and `B_DecryptFinal`. `B_DecryptFinal` returns `BE_INPUT_DATA` if the MAC does not match. You may pass `(B_ALGORITHM_OBJ)NULL_PTR` for all *randomAlgorithm* arguments.

Due to the nature of the RC4 algorithm, security is compromised if multiple data blocks are encrypted with the same RC4 key. Therefore, `B_EncryptUpdate` cannot be called after `B_EncryptFinal`. To begin an encryption operation for a new data block, you must call `B_EncryptInit` and supply a new key.

## Algorithm methods to include in application's algorithm chooser:

`AM_RC4_WITH_MAC_ENCRYPT` for encryption, or `AM_RC4_WITH_MAC_DECRYPT` for decryption.

## Key info types for *keyObject* in `B_EncryptInit` or `B_DecryptInit`:

`KI_Item` that gives the address and length of the RC4 key.

## Compatible representation:

`AI_RC4WithMAC_BER`.

## Output considerations:

The total number of output bytes from encryption will be *macLen* bytes more than the input.

## Token-based algorithm methods:



`AI_RC4WithMAC` may be used to access the hardware-related algorithm methods `AM_TOKEN_RC4_ENCRYPT` and `AM_TOKEN_RC4_DECRYPT`, for use with BHAPI.

## Token-based key info types:

When used with one of the hardware algorithm methods listed above, `AI_RC4WithMac` should be used with `KI-Token` or `KI_ExtendedToken`.

## AI\_RC4WithMAC\_BER

### Purpose:

This AI is similar to AI\_RC4WithMAC except that it uses the ASN.1 BER format. This AI allows you to parse and create ASN.1 algorithm identifiers such as used in PKCS #7 and other protocols. You call B\_SetAlgorithmInfo to initialize an algorithm object from the encoded algorithm identifier which includes ASN.1 encoding of the B\_RC4\_WITH\_MAC\_PARAMS structure defined in the description of AI\_RC4WithMAC. You call B\_GetAlgorithmInfo with this AI to create an encoded algorithm identifier from an algorithm object that was created using AI\_RC4WithMAC or AI\_RC4WithMAC\_BER. The OID for this algorithm, excluding the tag and length bytes, in decimal is "42, 134, 72, 134, 247, 13, 3, 5".

### Type of information this allows you to use:

the encoding of an algorithm identifier that specifies the RC4 With MAC encryption algorithm.

### Format of *info* supplied to B\_SetAlgorithmInfo:

pointer to an ITEM structure that gives the address and length of the BER-encoded algorithm identifier. The encoding is converted to DER before it is copied to the algorithm object. B\_SetAlgorithmInfo returns BE\_WRONG\_ALGORITHM\_INFO if the algorithm identifier specifies an algorithm other than RC4.

### Format of *info* returned by B\_GetAlgorithmInfo:

pointer to an ITEM structure that gives the address and length of the DER-encoded algorithm identifier.

### Crypto-C procedures to use with algorithm object:

B\_EncryptInit, B\_EncryptUpdate, B\_EncryptFinal, B\_DecryptInit, B\_DecryptUpdate, and B\_DecryptFinal. B\_DecryptFinal returns BE\_INPUT\_DATA if the MAC does not match. You may pass (B\_ALGORITHM\_OBJ)NULL\_PTR for all *randomAlgorithm* arguments.

Due to the nature of the RC4 algorithm, security is compromised if multiple data blocks are encrypted with the same RC4 key. Therefore, B\_EncryptUpdate cannot be called after B\_EncryptFinal. To begin an encryption operation for a new data block,

you must call `B_EncryptInit` and supply a new key.

### Algorithm methods to include in application's algorithm chooser:

`AM_RC4_WITH_MAC_ENCRYPT` for encryption or `AM_RC4_WITH_MAC_DECRYPT` for decryption.

### Key info types for *keyObject* in `B_EncryptInit` or `B_DecryptInit`:

`KI_Item` that gives the address and length of the RC4 key.

### Compatible representation:

`AI_RC4WithMAC`.

### Output considerations:

The total number of output bytes from encryption will be *macLen* bytes more than the input.

## AI\_RC5\_CBC

### Purpose:

This AI allows you to perform RC5 encryption and decryption in CBC mode with an 8-byte initialization vector and a variable number of rounds, as defined in RFC 2040. Since AI\_RC5\_CBC does not pad, the total number of input bytes must be a multiple of 8 bytes. See AI\_RC5\_CBCPad for the same algorithm with padding.

Other algorithms that can be used for encryption/decryption in CBC mode without padding are AI\_DES\_CBC\_IV8, AI\_DES\_EDE3\_CBC\_IV8, AI\_DESX\_CBC\_IV8, and AI\_RC2\_CBC.

### Type of information this allows you to use:

a version number, a rounds count, a word size, and an 8-byte initialization vector for the RC5 32/r/b CBC encryption algorithm.

**Note:** To implement RC5 with a word size other than 32 bits, you should use AI\_FeedbackCipher.

### Format of *info* supplied to B\_SetAlgorithmInfo:

pointer to an A\_RC5\_CBC\_PARAMS structure:

```
typedef struct {
    unsigned int  version,           /* currently 1.0 defined 0x10 */
    unsigned int  rounds;           /* number of rounds (0 - 255) */
    unsigned int  wordSizeInBits;   /* AI_RC5_CBC requires 32 */
    unsigned char *iv;              /* initialization vector (8 bytes) */
} A_RC5_CBC_PARAMS;
```

### Format of *info* returned by B\_GetAlgorithmInfo:

pointer to an A\_RC5\_CBC\_PARAMS structure (see above).

### Crypto-C procedures to use with algorithm object:

B\_EncryptInit, B\_EncryptUpdate, B\_EncryptFinal, B\_DecryptInit, B\_DecryptUpdate, and B\_DecryptFinal. You may pass (B\_ALGORITHM\_OBJ)NULL\_PTR for all *randomAlgorithm* arguments.

## Algorithm methods to include in application's algorithm chooser:

AM\_RC5\_CBC\_ENCRYPT for encryption and AM\_RC5\_CBC\_DECRYPT for decryption.

## Key info types for *keyObject* in B\_EncryptInit or B\_DecryptInit:

KI\_Item, that gives the address and length of the RC5 key.

## Input Constraints:

During encryption, this algorithm does not pad the output. Thus, you must provide input that is a multiple of 8 bytes.

## Token-based algorithm methods:



AI\_RC5\_CBC may be used to access the hardware-related (BHAPI) algorithm methods AM\_TOKEN\_RC5\_CBC\_ENCRYPT and AM\_TOKEN\_RC5\_CBC\_DECRYPT.

## Token-based key info types:

When used with one of the hardware algorithm methods listed above, AI\_RC5\_CBC should be used with KI\_Token or KI\_ExtendedToken.

## AI\_RC5\_CBCPad

### Purpose:

This AI allows you to perform RC5 encryption or decryption in CBC mode with an 8-byte initialization vector and a variable number of rounds, as defined in RFC 2040. This algorithm pads, so the input data does not have to be a multiple of 8 bytes.

Other algorithms that can be used for encryption/decryption in CBC mode with padding are AI\_DES\_CBCPadI V8, AI\_DES\_EDE3\_CBCPadI V8, AI\_DESX\_CBCPadI V8, and AI\_RC2\_CBCPad.

### Type of information this allows you to use:

a version number, a rounds count, a word size, and an 8-byte initialization vector for the RC5 32/r/b CBC encryption algorithm.

**Note:** To implement RC5 with a word size other than 32 bits, use AI\_FeedbackCipher.

### Format of *info* supplied to B\_SetAlgorithmInfo:

pointer to an A\_RC5\_CBC\_PARAMS structure:

```
typedef struct {
    unsigned int  version,                /* currently 1.0 defined 0x10 */
    unsigned int  rounds;                 /* number of rounds (0 - 255) */
    unsigned int  wordSizeInBits;        /* AI_RC5_CBCPad requires 32 */
    unsigned char *iv;                    /* initialization vector (8 bytes) */
} A_RC5_CBC_PARAMS;
```

### Format of *info* returned by B\_GetAlgorithmInfo:

pointer to an A\_RC5\_CBC\_PARAMS structure (see above).

### Crypto-C procedures to use with algorithm object:

B\_EncryptInit, B\_EncryptUpdate, B\_EncryptFinal, B\_DecryptInit, B\_DecryptUpdate, and B\_DecryptFinal. You may pass (B\_ALGORITHM\_OBJ) NULL\_PTR for all *randomAlgorithm* arguments.

**Algorithm methods to include in application's algorithm chooser:**

AM\_RC5\_CBC\_ENCRYPT for encryption and AM\_RC5\_CBC\_DECRYPT for decryption.

**Key info types for *keyObject* in B\_EncryptInit or B\_DecryptInit:**

KI\_1 tem, that gives the address and length of the RC5 key.

**Compatible representation:**

AI\_RC5\_CBCPadBER.

**Output considerations:**

During encryption, this AI pads the output. Thus, the total number of output bytes from encryption can be as many as 8 bytes more than the total output.

## AI\_RC5\_CBCPadBER

### Purpose:

This AI is similar to AI\_RC5\_CBCPad except that it uses the ASN.1 BER format. This AI allows you to parse and create ASN.1 algorithm identifiers such as those used in PKCS #7 and other protocols. You call `B_SetAlgorithmInfo` to initialize an algorithm object from the encoded algorithm identifier, which includes ASN.1 encoding of the `A_RC5_CBC_PARAMS` structure defined in the description of AI\_RC5\_CBCPad. You call `B_GetAlgorithmInfo` with this AI to create an encoded algorithm identifier from an algorithm object that was created using AI\_RC5\_CBCPad, AI\_RC5\_CBCPadBER or AI\_RC5\_CBCPadPEM. The OID for this algorithm, excluding the tag and length bytes, in decimal is "42, 134, 72, 134, 247, 13, 3, 9".

### Type of information this allows you to use:

the encoding of an algorithm identifier that specifies the RC5 32/r/b CBC encryption algorithm.

### Format of *info* supplied to `B_SetAlgorithmInfo`:

pointer to an ITEM structure that gives the address and length of the BER-encoded algorithm identifier. The encoding is converted to DER before it is copied to the algorithm object. `B_SetAlgorithmInfo` returns `BE_WRONG_ALGORITHM_INFO` if the algorithm identifier specifies an algorithm other than RC5-CBC With Padding.

### Format of *info* returned by `B_GetAlgorithmInfo`:

pointer to an ITEM structure that gives the address and length of the DER-encoded algorithm identifier.

### Crypto-C procedures to use with algorithm object:

`B_EncryptInit`, `B_EncryptUpdate`, `B_EncryptFinal`, `B_DecryptInit`, `B_DecryptUpdate`, and `B_DecryptFinal`. You may pass `(B_ALGORITHM_OBJ)NULL_PTR` for all *randomAlgorithm* arguments.

### Algorithm methods to include in application's algorithm chooser:

`AM_RC5_CBC_ENCRYPT` for encryption and `AM_RC5_CBC_DECRYPT` for decryption.

### **Key info types for *keyObject* in B\_EncryptInit or B\_DecryptInit:**

keyLength, which gives the address and length of the RC5 key.

### **Compatible representation:**

AI\_RC5\_CBCPad.

### **Output considerations:**

During encryption, this AI pads the output. Thus, the total number of output bytes from encryption can be as many as 8 bytes more than the total output.

## AI\_RESET\_IV

### Purpose:

This AI allows you to change the initialization vector (IV) for a cipher object created with `AI_FeedbackCipher` without the need to create a new algorithm object or bind in a new key. This increases the performance of applications that have a long-lived symmetric key (e.g., DES key) that is used to encrypt many blocks or messages, each of which has a unique IV.

A similar AI that can be used to change the IV of a CBC mode cipher is `AI_CBC_IV8`.

### Type of Information this allows you to use:

a new initialization vector to reset an encryption/decryption object defined with `AI_FeedbackCipher`.

### Format of *info* supplied to `B_SetAlgorithmInfo`

a pointer to an `ITEM` of length equal to the old initialization vector.

### Format of *info* returned by `B_GetAlgorithmInfo` returns

a pointer to an `ITEM`.

### Algorithm methods to include in chooser

none.

**Note:** Reinitialization may be done anytime after an encryption/decryption has been set with its algorithm info. It takes effect after the next initialization. It may be used in conjunction with a new key to start a new encryption/decryption session.

## AI\_RFC1113Recode

### Purpose:

This AI allows you to convert data from binary format to ASCII, and vice versa, as defined by RFC 1113.

### Type of information this allows you to use:

the binary to printable recoding algorithm as defined by RFC 1113; see also RFC 1421 for updated version of the standard.

### Format of *info* supplied to `B_SetAlgorithmInfo`:

NULL\_PTR.

### Format of *info* returned by `B_GetAlgorithmInfo`:

NULL\_PTR.

### Crypto-C procedures to use with algorithm object:

`B_EncodeInit`, `B_EncodeUpdate`, `B_EncodeFinal`, `B_DecodeInit`, `B_DecodeUpdate`, and `B_DecodeFinal`.

### Output considerations:

When encoding, for each 3 bytes of input there are 4 bytes of output. When decoding, for each 4 bytes of input there are 3 bytes of output.

## AI\_RSAStrongKeyGen

### Purpose:

This AI allows you to specify the parameters for generating an RSA public/private key pair as defined in PKCS #1. You may also use AI\_RSAStrongKeyGen to generate RSA key pairs.

### Type of information this allows you to use:

the parameters for generating an RSA public/private key pair as defined in PKCS #1, where the modulus size and public exponent are specified.

### Format of *info* supplied to B\_SetAlgorithmInfo:

pointer to an A\_RSA\_KEY\_GEN\_PARAMS structure:

```
typedef struct {
    unsigned int modulusBits;           /* size of modulus in bits */
    ITEM        publicExponent;        /* fixed public exponent */
} A_RSA_KEY_GEN_PARAMS;
```

The *publicExponent* ITEM supplies an integer in canonical format, where the ITEM's *data* points to an unsigned byte array -- most significant byte first -- and the ITEM's *len* gives its length. All leading zeros are stripped from the integer before it is copied to the algorithm object.

### Format of *info* returned by B\_GetAlgorithmInfo:

pointer to an A\_RSA\_KEY\_GEN\_PARAMS structure (see above). All leading zeros have been stripped from the *publicExponent* integer.

### Crypto-C procedures to use with algorithm object:

B\_GenerateInit and B\_GenerateKeyPair. B\_GenerateKeyPair sets the *publicKey* key object with the KI\_RSAPublic information and the *privateKey* key object with the KI\_PKCS\_RSAPrivate information. You must pass an initialized random algorithm to B\_GenerateKeyPair.

**Algorithm methods to include in application's algorithm chooser:**

AM\_RSA\_KEY\_GEN.

## AI\_RSAPrivate

### Purpose:

This AI allows you to encrypt data using the raw RSA algorithm. You can find the description of this algorithm in B. Schneier's *Applied Cryptography*.

AI\_RSAPrivate is different from AI\_PKCS\_RSAPrivate because the former allows you to encrypt raw data, while the latter encrypts data in PKCS #1 format.

Because this algorithm does not pad, the total number of input bytes must be a multiple of the key's modulus size in bytes. Your application is responsible for padding the data as appropriate. Also, each modulus-size block of input, interpreted as an integer with the most significant byte first, must be numerically less than the key's modulus. To do this, divide your data into blocks that are one byte smaller than the modulus, and prepend one byte of zeros to each block.

To perform RSA encryption you can also use AI\_PKCS\_RSAPrivate and AI\_SET\_OAEP\_RSAPrivate. But you can use AI\_RSAPrivate only if the data will be decrypted with AI\_RSAPublic.

### Type of information this allows you to use:

the RSA algorithm for performing raw private-key encryption.

### Format of *info* supplied to B\_SetAlgorithmInfo:

NULL\_PTR.

### Format of *info* returned by B\_GetAlgorithmInfo:

NULL\_PTR.

### Crypto-C procedures to use with algorithm object:

B\_EncryptInit, B\_EncryptUpdate, B\_EncryptFinal, B\_DecryptInit, B\_DecryptUpdate, and B\_DecryptFinal. You may pass (B\_ALGORITHM\_OBJ) NULL\_PTR for all *randomAlgorithm* arguments.

### Algorithm methods to include in application's algorithm chooser:

AM\_RSA\_CRT\_ENCRYPT or AM\_RSA\_CRT\_ENCRYPT\_BLIND for encryption, or

AM\_RSA\_CRT\_DECRYPT or AM\_RSA\_CRT\_DECRYPT\_BLIND for decryption.

AM\_RSA\_CRT\_ENCRYPT\_BLIND and AM\_RSA\_CRT\_DECRYPT\_BLIND perform blinding to protect against timing attacks, whereas AM\_RSA\_CRT\_ENCRYPT and AM\_RSA\_CRT\_DECRYPT does not.

### **Key info types for *keyObject* in B\_EncryptInit or B\_DecryptInit:**

KI\_RSA\_CRT, KI\_PKCS\_RSAPrivate, KI\_PKCS\_RSAPrivateBER, or KI\_RSAPrivateBSAFE1.

### **Input constraints:**

Because this algorithm does not pad, the total number of input bytes must be a multiple of the key's modulus size in bytes. Also, each modulus-size block of input, interpreted as an integer with the most significant byte first, must be numerically less than the key's modulus.

### **Token-based algorithm methods:**



AI\_RSAPrivate may include the hardware algorithm method AM\_TOKEN\_RSA\_CRT\_ENCRYPT or AM\_TOKEN\_RSA\_CRT\_DECRYPT in the algorithm chooser, for use with BHAPI.

### **Token-based key info types:**

When used with one of the hardware algorithm methods described, AI\_RSAPrivate should be used with KI\_Token or KI\_KeypairToken.

## AI\_RSAPrivateBSAFE1

### Purpose:

Deprecated. This AI is included only for backward compatibility.

### Type of information this allows you to use:

the encryption type parameter (pad, pad with checksum, or raw) for performing RSA private key encryption as defined by BSAFE 1.x.

### Format of *info* supplied to B\_SetAlgorithmInfo:

pointer to a B\_BSAFE1\_ENCRYPTI ON\_PARAMS structure:

```
typedef struct {
    int encrypti onType; /* encrypti on type */
} B_BSAFE1_ENCRYPTI ON_PARAMS;
```

*encrypti onType* should be set to B\_BSAFE1\_PAD for pad mode, B\_BSAFE1\_PAD\_CHECKSUM for pad with checksum mode, or B\_BSAFE1\_RAW for raw mode.

### Format of *info* returned by B\_GetAlgorithmInfo:

pointer to a B\_BSAFE1\_ENCRYPTI ON\_PARAMS structure (see above).

### Crypto-C procedures to use with algorithm object:

B\_EncryptI ni t, B\_EncryptUpdate, B\_EncryptFi nal , B\_DecryptI ni t, B\_DecryptUpdate, and B\_DecryptFi nal . Note that for pad mode or pad with checksum mode, B\_EncryptUpdate, and B\_EncryptFi nal require a random algorithm. You may pass (B\_ALGORI THM\_OBJ) NULL\_PTR for the *randomAlgori thm* argument in B\_DecryptUpdate and B\_DecryptFi nal .

### Notes:

If the input and output buffers of the RSA operation are interpreted as integers, the BSAFE 1.x format puts the least significant byte of the integer at the beginning of the buffer. This is in reverse order from algorithms in BSAFE 2.1 and above, such as AI\_RSAPri vate and AI\_PKCS\_RSAPri vate, which put the most significant byte of the

integer at the beginning of the buffer.

## Algorithm methods to include in application's algorithm chooser:

AM\_RSA\_CRT\_ENCRYPT or AM\_RSA\_CRT\_ENCRYPT\_BLI ND for encryption, or AM\_RSA\_CRT\_DECRYPT or AM\_RSA\_CRT\_DECRYPT\_BLI ND for decryption.

AM\_RSA\_CRT\_ENCRYPT\_BLI ND and AM\_RSA\_CRT\_DECRYPT\_BLI ND perform blinding to protect against timing attacks, whereas AM\_RSA\_CRT\_ENCRYPT and AM\_RSA\_CRT\_DECRYPT do not.

## Key info types for *keyObject* in B\_EncryptInit or B\_DecryptInit:

KI\_RSA\_CRT, KI\_PKCS\_RSAPri vate, KI\_PKCS\_RSAPri vateBER, or KI\_RSAPri vateBSAFE1.

## Input constraints:

In raw mode, the total number of input bytes must be a multiple of the key's modulus size in bytes. Also, each modulus-size block of input, interpreted as an integer with the most significant byte first, must be numerically less than the key's modulus.

## Output considerations:

In pad mode and in pad with checksum mode, the output can be as large as one block greater than the number of input blocks, where each block is the size of the key's modulus size in bytes. For instance, given a 512-bit (64-byte) key and input of 64 bytes or less (one block), the output can be either 64 or 128 bytes long. With input of more than 64 bytes but less than or equal to 128 (two blocks), the output can be either 128 or 192 bytes long.

## AI\_RSAPublic

### Purpose:

This AI allows you to decrypt data using the raw RSA algorithm. You can find the description of this algorithm in B. Schneier's *Applied Cryptography*.

AI\_RSAPublic is different from AI\_PKCS\_RSAPublic because the latter allows you to decrypt  $k-11$  bytes, where  $k$  is the size of the modulus in bytes, while you can use the former to decrypt up to  $k$  bytes. Note that it is the application's responsibility to strip the padding that was appended by the application to the data during encryption with AI\_RSAPrivate.

Because this algorithm does not pad, the total number of input bytes must be a multiple of the key's modulus size in bytes. Also, each modulus-size block of input, interpreted as an integer with the most significant byte first, must be numerically less than the key's modulus.

To perform RSA decryption you can also use AI\_PKCS\_RSAPublic and AI\_SET\_OAEP\_RSAPublic. But you can use AI\_RSAPublic only if the data has been encrypted with AI\_RSAPrivate.

### Type of information this allows you to use:

the RSA algorithm for performing raw public-key decryption.

### Format of *info* supplied to B\_SetAlgorithmInfo:

NULL\_PTR.

### Format of *info* returned by B\_GetAlgorithmInfo:

NULL\_PTR.

### Crypto-C procedures to use with algorithm object:

B\_EncryptInit, B\_EncryptUpdate, B\_EncryptFinal, B\_DecryptInit, B\_DecryptUpdate, and B\_DecryptFinal. You may pass (B\_ALGORITHM\_OBJ) NULL\_PTR for all *randomAlgorithm* arguments.

## Algorithm methods to include in application's algorithm chooser:

AM\_RSA\_ENCRYPT for encryption or AM\_RSA\_DECRYPT for decryption.

## Key info types for *keyObject* in B\_EncryptInit or B\_DecryptInit:

KI\_RSAPublic, KI\_RSAPublicBER, or KI\_RSAPublicBSAFE1.

## Input constraints:

Because this algorithm does not pad, the total number of input bytes must be a multiple of the key's modulus size in bytes. Also, each modulus-size block of input, interpreted as an integer with the most significant byte first, must be numerically less than the key's modulus.

## Token-based algorithm methods:



AI\_RSAPublic may include the hardware algorithm methods AM\_TOKEN\_RSA\_ENCRYPT, AM\_TOKEN\_RSA\_DECRYPT, and AM\_TOKEN\_RSA\_PUB\_DECRYPT in the algorithm chooser for use with BHAPI.

## Token-based key info types:

When used with one of the hardware algorithm methods described, AI\_RSAPublic should be used with KI\_Token or KI\_KeypairToken.

# AI\_RSAPublicBSAFE1

## Purpose:

Deprecated. This AI is included only for backward compatibility.

## Type of information this allows you to use:

the decryption type parameter (pad, pad with checksum, or raw) for performing RSA public key decryption as defined by BSAFE 1.x.

## Format of *info* supplied to B\_SetAlgorithmInfo:

pointer to a B\_BSAFE1\_ENCRYPTI ON\_PARAMS structure:

```
typedef struct {
    int encrypti onType; /* encrypti on type */
} B_BSAFE1_ENCRYPTI ON_PARAMS;
```

*encrypti onType* should be set to B\_BSAFE1\_PAD for pad mode, B\_BSAFE1\_PAD\_CHECKSUM for pad with checksum mode, or B\_BSAFE1\_RAW for raw mode.

## Format of *info* returned by B\_GetAlgorithmInfo:

pointer to a B\_BSAFE1\_ENCRYPTI ON\_PARAMS structure (see above).

## Crypto-C procedures to use with algorithm object:

B\_EncryptI ni t, B\_EncryptUpdate, B\_EncryptFi nal , B\_DecryptI ni t, B\_DecryptUpdate, and B\_DecryptFi nal . Note that for pad mode or pad with checksum mode, B\_EncryptUpdate and B\_EncryptFi nal require a random algorithm. You may pass (B\_ALGORI THM\_OBJ)NULL\_PTR for the *randomAlgori thm* argument in B\_DecryptUpdate and B\_DecryptFi nal .

## Notes:

If the input and output buffers of the RSA operation are interpreted as integers, the BSAFE 1.x format puts the least significant byte of the integer at the beginning of the buffer. This is in reverse order from algorithms in BSAFE 2.1 and above, such as AI\_RSAPubl i c and AI\_PKCS\_RSAPubl i c, which put the most significant byte of the

integer at the beginning of the buffer.

### **Algorithm methods to include in application's algorithm chooser:**

AM\_RSA\_ENCRYPT for encryption or AM\_RSA\_DECRYPT for decryption.

### **Key info types for *keyObject* in B\_EncryptInit or B\_DecryptInit:**

KI\_RSAPublic, KI\_RSAPublicBER, or KI\_RSAPublicBSAFE1.

### **Input constraints:**

In raw mode, the total number of input bytes must be a multiple of the key's modulus size in bytes. Also, each modulus-size block of input, interpreted as an integer with the most significant byte first, must be numerically less than the key's modulus.

### **Output considerations:**

In pad mode and in pad with checksum mode, the output can be as large as one block greater than the number of input blocks, where each block is the size of the key's modulus size in bytes. For instance, given a 512-bit (64-byte) key and input of 64 bytes or less (one block), the output can be either 64 or 128 bytes long. With input of more than 64 bytes but less than or equal to 128 (two blocks), the output can be either 128 or 192 bytes long.

# AI\_RSAStrongKeyGen

## Purpose:

This AI allows you to specify the parameters for generating an RSA public/private key pair as defined in PKCS #1. The moduli generated are in conformance with the strength criteria of the ANSI X9.31 Draft. If this conformance is not desired, you may use a faster AI\_RSAStrongKeyGen to generate RSA key pairs.

## Type of information this allows you to use:

the parameters for generating an RSA public/private key pair as defined in PKCS #1, where the modulus size and public exponent are specified. The moduli generated are in conformance with the strength criteria of the ANSI X9.31 Draft.

## Format of *info* supplied to B\_SetAlgorithmInfo:

pointer to an A\_RSA\_KEY\_GEN\_PARAMS structure:

```
typedef struct {
    unsigned int modulusBits;           /* size of modulus in bits */
    ITEM publicExponent;                 /* fixed public exponent */
} A_RSA_KEY_GEN_PARAMS;
```

The *publicExponent* ITEM supplies an integer in canonical format, where the ITEM's *data* points to an unsigned byte array, most significant byte first and the ITEM's *len* gives its length. All leading zeros are stripped from the integer before it is copied to the algorithm object. *modulusBits* must be at least 512 and must be a multiple of 16.

## Format of *info* returned by B\_GetAlgorithmInfo:

pointer to an A\_RSA\_KEY\_GEN\_PARAMS structure (see above). All leading zeros have been stripped from the *publicExponent* integer.

## Crypto-C procedures to use with algorithm object:

B\_GenerateInit and B\_GenerateKeypair. B\_GenerateKeypair sets the *publicKey* key object with the KI\_RSAPublic information and the *privateKey* key object with the KI\_PKCS\_RSAPrivate information. You must pass an initialized random algorithm to B\_GenerateKeypair.

**Algorithm methods to include in application's algorithm chooser:**

AM\_RSA\_STRONG\_KEY\_GEN.

## AI\_SET\_OAEP\_RSAPrivate

### Purpose:

This AI allows you to decrypt data encrypted using AI\_SET\_OAEP\_RSAPublic. This algorithm is used by the Secure Electronic Transaction (SET) protocol defined by Visa and MasterCard in the SET 1.0 specification released August 1, 1996. It replaces PKCS #1 v1.5 padding with a form of Optimal Asymmetric Encryption Padding (OAEP) that was developed for the SET protocol. OAEP provides protection against cryptanalytic attacks on the padding algorithm which are possible when most of the message being encrypted is known to the attacker. A more standard form of OAEP is now part of version 2.0 of the PKCS #1 standard and is implemented by AI\_PKCS\_OAEP\_RSAPrivate and AI\_PKCS\_OAEP\_RSAPublic.

### Type of information this allows you to use:

the RSA algorithm for performing private key decryption following the OAEP procedure outlined in the Aug. 1, 1996 version of the SET specifications.

### Format of *info* supplied to B\_SetAlgorithmInfo:

NULL\_PTR.

### Format of *info* returned by B\_GetAlgorithmInfo:

NULL\_PTR.

### Crypto-C procedures to use with algorithm object:

B\_EncryptInit, B\_EncryptUpdate, and B\_EncryptFinal for encryption, and B\_DecryptInit, B\_DecryptUpdate, and B\_DecryptFinal for decryption. B\_EncryptUpdate and B\_EncryptFinal require a random algorithm. You may pass (B\_ALGORITHM\_OBJ) NULL\_PTR for the *randomAlgorithm* argument in B\_DecryptUpdate and B\_DecryptFinal.

### Algorithm methods to include in application's algorithm chooser:

AM\_RSA\_CRT\_ENCRYPT or AM\_RSA\_CRT\_ENCRYPT\_BLIND for encryption and AM\_RSA\_CRT\_DECRYPT or AM\_RSA\_CRT\_DECRYPT\_BLIND for decryption. AM\_RSA\_CRT\_ENCRYPT\_BLIND and AM\_RSA\_CRT\_DECRYPT\_BLIND will perform blinding to protect against timing attacks, whereas AM\_RSA\_CRT\_ENCRYPT and

AM\_RSA\_CRT\_DECRYPT do not.

## Key info types for *keyObject* in B\_EncryptInit or B\_DecryptInit:

KI\_RSA\_CRT, KI\_PKCS\_RSAPrivate, KI\_PKCS\_RSAPrivateBER, or KI\_RSAPrivateBSAFE1.

## Input considerations:

The key size, in bits, must be a multiple of 8. For instance, 1024 is a valid key size; 1030 is not.

If encrypting, the total number of bytes to encrypt must be 25 fewer than the key size in bytes. For instance, with a 1024-bit key (128-bytes) the input must be 103-bytes (128 - 25). The SET standard calls for the input data to follow a particular format. The first byte is the block content (BC) and the following bytes are the actual data bytes (ADB). This AI does not check whether those bytes adhere to the SET specifications.

## Output considerations:

The output of encryption will be the same size as the key's modulus. The output of decryption will be 25 bytes fewer than the key size in bytes.

## AI\_SET\_OAEP\_RSAPublic

### Purpose:

This AI allows you to encrypt data which will be decrypted using AI\_SET\_OAEP\_RSAPrivate. This algorithm is used by the Secure Electronic Transaction (SET) protocol defined by Visa and MasterCard in the SET 1.0 specification released August 1, 1996. It replaces PKCS #1 v1.5 padding with a form of Optimal Asymmetric Encryption Padding (OAEP) that was developed for the SET protocol. OAEP provides protection against cryptanalytic attacks on the padding algorithm which are possible when most of the message being encrypted is known to the attacker. A more standard form of OAEP is now part of version 2.0 of the PKCS #1 standard and is implemented by AI\_PKCS\_OAEP\_RSAPrivate and AI\_PKCS\_OAEP\_RSAPublic.

### Type of information this allows you to use:

the RSA algorithm for performing public key encryption following the OAEP procedure outlined in the Aug. 1, 1996 version of the SET specifications.

### Format of *info* supplied to B\_SetAlgorithmInfo:

NULL\_PTR.

### Format of *info* returned by B\_GetAlgorithmInfo:

NULL\_PTR.

### Crypto-C procedures to use with algorithm object:

B\_EncryptInit, B\_EncryptUpdate, B\_EncryptFinal, B\_DecryptInit, B\_DecryptUpdate, and B\_DecryptFinal. B\_EncryptUpdate and B\_EncryptFinal require a random algorithm. You may pass (B\_ALGORITHM\_OBJ) NULL\_PTR for the *randomAlgorithm* argument in B\_DecryptUpdate and B\_DecryptFinal.

### Algorithm methods to include in application's algorithm chooser:

AM\_RSA\_ENCRYPT for encryption and AM\_RSA\_DECRYPT for decryption.

### Key info types for *keyObject* in B\_EncryptInit or B\_DecryptInit:

KI\_RSAPublic, KI\_RSAPublicBER, or KI\_RSAPublicSAFE1.

### **Input considerations:**

The key size in bits must be a multiple of 8; e.g., 1024 is a valid key size whereas 1030 is not.

If encrypting, the total number of bytes to encrypt must be 25 fewer than the key size in bytes. For instance, with a 1024-bit key (128-bytes) the input must be 103 bytes (128 - 25). The SET standard calls for the input data to follow a particular format. The first byte is the block content (BC) and the following bytes are the actual data bytes (ADB). This AI does not check whether those bytes adhere to the SET specifications.

### **Output considerations:**

The output of encryption will be the same size as the key's modulus. The output of decryption will be 25 bytes fewer than the key size in bytes.

# AI\_SHA1

## Purpose:

This AI allows you to create a message digest using the SHA1 digest algorithm as defined in FIPS PUB 180-1. This algorithm processes input data 64 bytes at a time but the length of the input does not have to be a multiple of 64 as the algorithm pads automatically.

The primary use for this AI is to authenticate data. Other algorithms that can be used for message digesting are AI\_MD2 and AI\_MD5 and their variants.

## Type of information this allows you to use:

the 20-byte SHA1 message digest algorithm as defined in FIPS PUB 180-1.

## Format of *info* supplied to B\_SetAlgorithmInfo:

NULL\_PTR.

## Format of *info* returned by B\_GetAlgorithmInfo:

NULL\_PTR.

## Crypto-C procedures to use with algorithm object:

B\_DigestInit, B\_DigestUpdate, and B\_DigestFinal. Supply NULL\_PTR for the *keyObject* argument in B\_DigestInit.

## Algorithm methods to include in application's algorithm chooser:

AM\_SHA.

## Compatible representation:

AI\_SHA1\_BER

## Output considerations:

The output of B\_DigestFinal will be 20 bytes long.

## AI\_SHA1\_BER

### Purpose:

This AI is similar to AI\_SHA1 except that it uses the ASN.1 BER format. This AI allows you to parse and create ASN.1 algorithm identifiers such as used in PKCS #7 and other protocols. You call B\_SetAlgorithmInfo to initialize an algorithm object from the encoded algorithm identifier. You call B\_GetAlgorithmInfo with this AI to create an encoded algorithm identifier from an algorithm object that was created using AI\_SHA1 or AI\_SHA1\_BER. The OID for this algorithm, excluding the tag and length bytes, in decimal is "43, 14, 3, 2, 26".

### Type of information this allows you to use:

the encoding of an algorithm identifier that specifies the SHA1 message digest algorithm as defined in FIPS PUB 180-1.

### Format of *info* supplied to B\_SetAlgorithmInfo:

pointer to an ITEM structure that gives the address and length of the BER-encoded algorithm identifier. The encoding is converted to DER before it is copied to the algorithm object. B\_SetAlgorithmInfo returns BE\_WRONG\_ALGORITHM\_INFO if the algorithm identifier specifies a message digest algorithm other than SHA1.

### Format of *info* returned by B\_GetAlgorithmInfo:

pointer to an ITEM structure that gives the address and length of the DER-encoded algorithm identifier.

### Crypto-C procedures to use with algorithm object:

B\_DigestInit, B\_DigestUpdate, and B\_DigestFinal. Supply NULL\_PTR for the *keyObject* argument in B\_DigestInit.

### Algorithm methods to include in application's algorithm chooser:

AM\_SHA.

### Compatible representation:

AI\_SHA1

## Output considerations:

The output of `B_DigestFinal` will be 20 bytes long.

## AI\_SHA1Random

### Purpose:

This AI allows you to generate a stream of pseudo-random numbers which are guaranteed to have a very high degree of randomness. Random numbers are used in deriving public and private keys, initialization vectors, etc. This AI uses SHA1 as an underlying hashing function. The details of this algorithm are available from RSA Laboratories' Bulletin #8 or online at <http://www.rsa.com/rsalabs/html/bulletins.html>.

Other algorithms that can be used to generate pseudo-random numbers are AI\_MD2Random, AI\_MD5Random, and AI\_X962Random\_V0.

### Notes:

In this API, AI\_SHA1Random is identical to AI\_X962Random\_V0 (Section 2.97); however, this identification may change in future versions of Crypto-C. For forward compatibility, we recommend that you do not use the name AI\_SHA1Random in your applications; use AI\_X962Random\_V0 instead.

AI\_X962Random\_V0 provides an implementation of SHA-1 Random that is based on the X9.62 Draft standard; this is different from the implementation of SHA-1 Random in RSA Data Security, Inc.'s Java cryptographic toolkit, RSA BSAFE Crypto-J. Future versions of Crypto-C may implement AI\_SHA1Random in a manner compatible with the implementation provided via the "SHA1Random" value passed to the JSAFE\_SecureRandom class in Crypto-J.

## AI\_SHA1WithDES\_CBCPad

### Purpose:

This AI allows you to perform password-based encryption. This means that the input data will be encrypted with a secret key derived from a password, and it can be successfully decrypted only when the correct password is provided. Although this AI can be used to encrypt arbitrary data, its intended primary use is for encrypting private keys when transferring them from one computer system to another, as described in PKCS #8.

This AI employs DES secret-key encryption in cipher-block chaining (CBC) mode with padding, where the secret key is derived from a password using the SHA1 message digest algorithm. The details of this algorithm are contained in PKCS #5. DES is defined in FIPS PUB 81, and CBC mode of DES is defined in FIPS PUB 46-1. FIPS PUB 180-1 describes SHA1.

Other algorithms that can be used for password-based encryption are AI\_MD2WithDES\_CBCPad, AI\_MD2WithRC2\_CBCPad, AI\_MD5WithRC2\_CBCPad, and AI\_MD5WithDES\_CBCPad.

### Type of information this allows you to use:

the salt and iteration count for the SHA1 With DES-CBC password-based encryption algorithm. The salt is concatenated with the password before being digested by SHA1, and the iteration count specifies how many times the digest needs to be run. The count of 2 indicates that the result of digesting password-and-salt string needs to be run once more through SHA1. The first 8 bytes of the final digest become the secret key for the DES cipher after being adjusted for parity as required by FIPS PUB 81, the next 8 bytes become the initialization vector, and the last 4 bytes are ignored.

### Format of *info* supplied to B\_SetAlgorithmInfo:

pointer to a B\_PBE\_PARAMS structure:

```
typedef struct {
    unsigned char *salt;           /* pointer to 8-byte salt value */
    unsigned int  iterationCount; /* iteration count */
} B_PBE_PARAMS;
```

RSA Data Security, Inc. recommends a minimum iteration count of 1,000. However,

for an additional byte or two of security the iteration should be  $2^8$  to  $2^{16}$ .

### Format of *info* returned by `B_GetAlgorithmInfo`:

pointer to a `B_PBE_PARAMS` structure (see above).

### Crypto-C procedures to use with algorithm object:

`B_EncryptInit`, `B_EncryptUpdate`, `B_EncryptFinal`, and `B_DecryptInit`, `B_DecryptUpdate`, and `B_DecryptFinal`. You may pass `(B_ALGORITHM_OBJ)NULL_PTR` for all *randomAlgorithm* arguments.

### Algorithm methods to include in application's algorithm chooser:

`AM_SHA` and `AM_DES_CBC_ENCRYPT` for encryption or `AM_DES_CBC_DECRYPT` for decryption.

### Key info types for *keyObject* in `B_EncryptInit` or `B_DecryptInit`:

`KI_Item` that gives the address and length of the password.

### Compatible representation:

`AI_SHA1WithDES_CBCPadBER`.

### Output considerations:

During encryption, this AI pads the output (which DES requires to be a multiple of 8 bytes long). Thus, the total number of output bytes from encryption can be as many as 8 bytes more than the total output.

## AI\_SHA1WithDES\_CBCPadBER

### Purpose:

This AI is similar to AI\_SHA1WithDES\_CBCPad except that it uses the ASN.1 BER format. This AI allows you to parse and create ASN.1 algorithm identifiers such as those used in PKCS #7 and other protocols. You call B\_SetAlgorithmInfo to initialize an algorithm object from the encoded algorithm identifier which includes ASN.1 encoding of the B\_PBE\_PARAMS structure defined in the description of AI\_SHA1WithDES\_CBCPad. You call B\_GetAlgorithmInfo with this AI to create an encoded algorithm identifier from an algorithm object that was created using AI\_SHA1WithDES\_CBCPad or AI\_SHA1WithDES\_CBCPad. The OID for this algorithm, excluding the tag and length bytes, in decimal is "42, 134, 72, 134, 247, 13, 1, 5, 10".

### Type of information this allows you to use:

the encoding of an algorithm identifier that specifies the SHA1 With DES-CBC password-based encryption algorithm, as defined by RSA Data Security, Inc.

### Format of *info* supplied to B\_SetAlgorithmInfo:

pointer to an ITEM structure that gives the address and length of the BER-encoded algorithm identifier. The encoding is converted to DER before it is copied to the algorithm object. B\_SetAlgorithmInfo returns BE\_WRONG\_ALGORITHM\_INFO if the algorithm identifier specifies an algorithm other than SHA1 With DES-CBC.

### Format of *info* returned by B\_GetAlgorithmInfo:

pointer to an ITEM structure that gives the address and length of the DER-encoded algorithm identifier.

### Crypto-C procedures to use with algorithm object:

B\_EncryptInit, B\_EncryptUpdate, B\_EncryptFinal, B\_DecryptInit, B\_DecryptUpdate, and B\_DecryptFinal. You may pass (B\_ALGORITHM\_OBJ)NULL\_PTR for all *randomAlgorithm* arguments.

### Algorithm methods to include in application's algorithm chooser:

AM\_SHA and AM\_DES\_CBC\_ENCRYPT for encryption or AM\_DES\_CBC\_DECRYPT for

decryption.

### **Key info types for *keyObject* in B\_EncryptInit or B\_DecryptInit:**

keyInfoItem that gives the address and length of the password.

### **Compatible representation:**

AI\_SHA1WithDES\_CBCPad.

### **Output considerations:**

During encryption, this AI pads the output (which DES requires to be a multiple of 8 bytes long). Thus, the total number of output bytes from encryption can be as many as 8 bytes more than the total output.

## AI\_SHA1WithRSAEncryption

### Purpose:

This AI allows you to perform signature operations that involve the SHA1 digest algorithm and RSA public key algorithm. The digest of a message is created using the SHA1 algorithm and then it is signed using PKCS#1 digital signature algorithm.

Other algorithms that can be used for the same purpose are

AI\_MD2WithRSAEncryption and AI\_MD5WithRSAEncryption.

### Type of information this allows you to use:

RSA Data Security, Inc.'s SHA1 With RSA signature algorithm that uses the SHA1 digest algorithm and RSA to create and verify RSA digital signatures as defined in PKCS #1.

Note that in order to perform PKCS #1 digital signatures with a 20-byte digest, the RSA key must be at least 368 bits long.

### Format of *info* supplied to B\_SetAlgorithmInfo:

NULL\_PTR.

### Format of *info* returned by B\_GetAlgorithmInfo:

NULL\_PTR.

### Crypto-C procedures to use with algorithm object:

B\_SignInit, B\_SignUpdate, B\_SignFinal, B\_VerifyInit, B\_VerifyUpdate, and B\_VerifyFinal. You may pass (B\_ALGORITHM\_OBJ) NULL\_PTR for all *randomAlgorithm* arguments.

### Algorithm methods to include in application's algorithm chooser:

AM\_MD2, and AM\_RSA\_CRT\_ENCRYPT, AM\_RSA\_CRT\_ENCRYPT\_BLIND, or AM\_RSA\_ENCRYPT, for signature creation; and AM\_RSA\_DECRYPT for signature verification.

AM\_RSA\_CRT\_ENCRYPT\_BLIND performs blinding to protect against timing attacks, whereas AM\_RSA\_CRT\_ENCRYPT does not.

### Key info types for *keyObject* in `B_SignInit`:

KI\_RSA\_CRT, KI\_PKCS\_RSAPrivate, KI\_PKCS\_RSAPrivateBER, KI\_RSAPrivate or KI\_RSAPrivateBSAFE1. Unless you use KI\_RSA\_CRT for your KI, you must include AM\_RSA\_ENCRYPT in your application's algorithm chooser.

### Key info types for *keyObject* in `B_VerifyInit`:

KI\_RSAPublic, KI\_RSAPublicBER or KI\_RSAPublicBSAFE1.

### Compatible representation:

AI\_SHA1WithRSAEncryptionBER.

### Output considerations:

The *signature* result of `B_SignFinal` will be the same size as the RSA key's modulus.

### Notes:

Although the RSA signature operation is called “encryption” and the verification operation is called “decryption”, the signer uses the digest and the private key and follows the steps needed to decrypt, while the verifier uses the transmitted digest and the public key and follows the steps needed to encrypt.

## AI\_SHA1WithRSAEncryptionBER

### Purpose:

This AI is similar to AI\_SHA1WithRSAEncryption except that it uses the ASN.1 BER format. This AI allows you to parse and create ASN.1 algorithm identifiers such as those used in PKCS #7 and other protocols. You call B\_SetAlgorithmInfo to initialize an algorithm object from the encoded algorithm identifier. You call B\_GetAlgorithmInfo with this AI to create an encoded algorithm identifier from an algorithm object that was created using AI\_SHA1WithRSAEncryption or AI\_SHA1WithRSAEncryptionBER. The OID for this algorithm, excluding the tag and length bytes, in decimal is "42, 134, 72, 134, 247, 13, 1, 1, 5".

### Type of information this allows you to use:

the encoding of an algorithm identifier that specifies RSA Data Security, Inc.'s SHA1 With RSA signature algorithm that uses the SHA1 digest algorithm and RSA to create and verify RSA digital signatures as defined in PKCS #1.

Note that in order to perform PKCS #1 digital signatures with a 20-byte digest, the RSA key must be at least 368 bits long.

### Format of *info* supplied to B\_SetAlgorithmInfo:

pointer to an ITEM structure that gives the address and length of the BER-encoded algorithm identifier. The encoding is converted to DER before it is copied to the algorithm object. B\_SetAlgorithmInfo returns BE\_WRONG\_ALGORITHM\_INFO if the algorithm identifier specifies an algorithm other than SHA1 With RSA Encryption.

### Format of *info* returned by B\_GetAlgorithmInfo:

pointer to an ITEM structure that gives the address and length of the DER-encoded algorithm identifier.

### Crypto-C procedures to use with algorithm object:

B\_SignInit, B\_SignUpdate, B\_SignFinal, B\_VerifyInit, B\_VerifyUpdate, and B\_VerifyFinal. You may pass (B\_ALGORITHM\_OBJ)NULL\_PTR for all *randomAlgorithm* arguments.

## Algorithm methods to include in application's algorithm chooser:

AM\_MD2, and AM\_RSA\_CRT\_ENCRYPT, AM\_RSA\_CRT\_ENCRYPT\_BLI ND, or AM\_RSA\_ENCRYPT, for signature creation; and AM\_RSA\_DECRYPT for signature verification.

AM\_RSA\_CRT\_ENCRYPT\_BLI ND performs blinding to protect against timing attacks, whereas AM\_RSA\_CRT\_ENCRYPT does not.

## Key info types for *keyObject* in B\_SignInit:

KI\_RSA\_CRT, KI\_PKCS\_RSAPri vate, KI\_PKCS\_RSAPri vateBER, KI\_RSAPri vate or KI\_RSAPri vateBSAFE1. Unless you use KI\_RSA\_CRT for your KI, you must include AM\_RSA\_ENCRYPT in your application's algorithm chooser.

## Key info types for *keyObject* in B\_VerifyInit:

KI\_RSAPubl i c, KI\_RSAPubl i cBER, or KI\_RSAPubl i cBSAFE1.

## Compatible representation:

AI\_SHA1Wi thRSAEncrypti on.

## Output considerations:

The *signature* result of B\_Si gnFi nal will be the same size as the RSA key's modulus.

## Notes:

Although the RSA signature operation is called “encryption” and the verification operation is called “decryption”, the signer uses the digest and the private key and follows the steps needed to decrypt, while the verifier uses the transmitted digest and the public key and follows the steps needed to encrypt.

## AI\_SignVerify

### Purpose:

This AI allows you to sign a message in compliance with the X9.31 Draft standard, or to verify X9.31 Draft compliant signatures.

### Type of information this allows you to use:

an RSA private key to sign a message in compliance with the X9.31 Draft standard, or an RSA public key to verify X9.31 Draft compliant signatures. For keys with even public exponent that were created with AI\_RSAStrongKeyGen, uses the Rabin-Williams algorithm as in X9.31 Draft.

### Format of *info* supplied to B\_SetAlgorithmInfo:

a pointer to a B\_SIGN\_VERIFY\_PARAMS structure:

```
typedef struct {
    /* Current Choices */
    unsigned char *encryptIonMethodName; /* "rsaSignX931", "rsaVerifyX931" */
    POINTER      encryptIonParams; /* Null for what is currently available*/
    unsigned char *digestMethodName; /* "sha1" */
    POINTER      digestParams; /* Null for sha1 */
    unsigned char *formatMethodName; /*"formatX931" */
    POINTER      formatParams; /* structure of type A_X931_PARAMS for sha1 */
} B_SIGN_VERIFY_PARAMS;
```

If *formatMethodName* is "formatX931", *formatParams* must be given a pointer to a structure of type A\_X931\_PARAMS:

```
typedef struct {
    unsigned int blockLen;
    unsigned int oidNum;
} A_X931_PARAMS;
```

### Format of *info* returned by B\_GetAlgorithmInfo:

a pointer to a B\_SIGN\_VERIFY\_PARAMS structure.

## Crypto-C procedures to use with algorithm object:

B\_Si gnI ni t, B\_Si gnUpdate, B\_Si gnFi nal , B\_Veri fyI ni t, B\_Veri fyUpdate, and B\_Veri fyFi nal . You may pass (B\_ALGORI THM\_OBJ)NULL\_PTR for all *randomAlgori thm* arguments.

## Algorithm methods to include in application's algorithm chooser:

AM\_SHA, AM\_FORMAT\_X931, and AM\_RSA\_CRT\_X931\_ENCRYPT for signature creation; or AM\_SHA, AM\_EXTRACT\_X931, and AM\_RSA\_X931\_DECRYPT for signature verification.

## Key info types for *keyObject* in B\_SignInit or B\_VerifyInit:

KI\_RSAPri vate or compatible key types to create a signature, or KI\_RSAPubl ic or compatible key types to verify a signature.

## AI\_SymKeyTokenGen



### Purpose:

This AI allows you to generate the token form of a symmetric-cipher key.

### Type of information this allows you to use:

the parameters for generating the token form of a symmetric key. The BSAFE Hardware API supports token forms of DES, RC2, RC4, RC5, and TDES keys.

### Format of *info* supplied to B\_SetAlgorithmInfo:

pointer to an A\_SYMMETRIC\_KEY\_SPECIFIER structure:

```
typedef struct {
    unsigned int    keyUsage;                /* X509 key usage bit map */
    unsigned int    keyLengthInBytes;
    unsigned long   lifetime;                /* Key lifetime; under consideration */
    unsigned int    protectFlag;             /* Store key in encrypted form */
    unsigned char   *cipherName;            /* String tag for key's cipher class */
                                                    /* , eg, "des" */
} A_SYMMETRIC_KEY_SPECIFIER;
```

where *cipherName* is one of: "des", "desx", "rc2", "rc4", "rc5", or "tripledes".

### Format of *info* returned by B\_GetAlgorithmInfo:

pointer to an A\_SYMMETRIC\_KEY\_SPECIFIER structure.

### Crypto-C procedures to use with algorithm object:

B\_SymmetricKeyGenerateInit and B\_SymmetricKeyGenerate.

### Algorithm methods to include in application's algorithm chooser:

AM\_SYMMETRIC\_KEY\_TOKEN\_GEN

### Notes:

Can only be used in conjunction with a hardware implementation; if no hardware

implementation is present, AI\_SymKeyTokenGen does not do anything.

AI\_SymKeyTokenGen can only be used if you have called B\_CreateSessionChooser for your application.

The corresponding software-based method is a HW\_TABLE\_ENTRY SF\_SYMMETRIC\_KEY\_TOKEN\_GEN. This provides software support in the case that hardware is unavailable. This method can be utilized only by including inside the hardware chooser table.

# AI\_X931Random

## Purpose:

This AI allows you to generate random numbers for RSA key generation in conformance with ANSI X9.31 standard. This AI can be used to supply multiple independent streams of randomness. It is included in Crypto-C mainly to satisfy the requirements of independent generation of large and private prime factors, as specified by ANSI X9.31 standard.

This AI is intended for use with AI\_RSAStrongKeyGen only. The SHA-1 based pseudo-random number generator, *G(sha1)*, that is defined in the X9.31 standard and in the FIPS182-1 DSA standard, is available as AI\_X962Random\_V0. If you are not using X9.31 rDSA signatures but require the *G(sha1)* hash function you should use AI\_X962Random\_V0 and not AI\_X931Random.

## Type of information this allows you to use:

A SHA-1 based pseudo-random number generator as defined in Appendix A of the X9.31 standard.

## Format of info supplied to B\_SetAlgorithmInfo:

NULL\_PTR, if there is only one stream and no additional seeding is desired,

or

a pointer to an A\_X931\_RANDOM\_PARAMS structure:

```
typedef struct
{
    unsigned int numberOfStreams;          /* number of independent streams */
    ITEM          seed;                      /* additional seeding */
} A_X931_RANDOM_PARAMS; /* to be equally divided among the streams */
```

When AI\_X931Random is used with AI\_RSAStrongKeyGen, the *numberOfStreams* field must always be equal to 6.

## Format of info returned by B\_GetAlgorithmInfo:

returns a NULL\_PTR if set with NULL\_PTR; returns a pointer to an

A\_X931\_RANDOM\_PARAMS structure otherwise.

### **BSAFE procedures to use with algorithm object:**

B\_RandomInit, B\_RandomUpdate, and B\_GenerateRandomBytes, and as the *randomAlgorithm* argument to other procedures.

### **Algorithm methods to include in application's algorithm chooser:**

AM\_X931\_RANDOM.

## AI\_X962Random\_V0

### Purpose:

This AI allows you to generate a stream of pseudo-random numbers which are guaranteed to have a very high degree of randomness. Random numbers are used in deriving public and private keys, initialization vectors, etc. This AI uses SHA1 as an underlying hashing function. The details of this algorithm are specified in the American National Standard X9.62-1997 Draft and it is similar to the algorithm in section A.2.1 of X9.31-1997 Draft.

This algorithm can produce numbers between zero and the value of a given prime minus one. Such numbers are useful for the US Government Digital Signature Standard.

Other algorithms that can be used to generate pseudo-random numbers are AI\_MD2Random, AI\_SHA1Random, and AI\_MD5Random.

### Type of information this allows you to use:

the SHA-1 pseudo-random generator as defined in the X9.62 Draft standard.

### Format of *info* supplied to B\_SetAlgorithmInfo:

NULL\_PTR, if it is desired to use the AI\_X962Random\_V0 object in the same fashion as AI\_MD5Random.

a pointer to an A\_SHA\_RANDOM\_PARAMS struct:.

```
typedef struct {
    ITEM prime;          /* Optional input for X-9.62 mode only. Used to */
                        /* generate a pseudo-random number (but not uniform) */
                        /* in [1, prime - 1]. Set prime.len to zero otherwise */
    ITEM seed;         /* Special additional seeding of 20 to 128 bytes long. */
                        /* May be used in place of usual B_UpdateRandom seeding calls, */
                        /* but requires the availability of nearly perfectly random bytes. */
                        /* If B_UpdateRandom seeding calls are used, then */
                        /* this additional seeding material is used to augment the */
                        /* randomness of the pseudo-random numbers generated. */
} A_SHA_RANDOM_PARAMS;
```

## Format of *info* returned by B\_GetAlgorithmInfo:

returns a NULL\_PTR if set with NULL\_PTR; otherwise, returns a pointer to an A\_SHA\_RANDOM\_PARAMS structure.

## Crypto-C procedures to use with algorithm object:

B\_RandomInit, B\_RandomUpdate, and B\_GenerateRandomBytes, and as the *randomAlgorithm* argument to other procedures.

## Algorithm methods to include in application's algorithm chooser:

AM\_SHA\_RANDOM.

## Notes:

There are a number of possible implementations of SHA-1 pseudo random number generation. AI\_X962Random\_V0 implements an SHA-1 Random generator that is based on the X9.62 Draft standard. The FIPS 186 standard defines a similar algorithm (also defined in X9.31 Draft), but due to slight differences between FIPS 186 and X9.62 Draft, the same seeding sequence will produce different outputs. In addition, AI\_X962Random\_V0's implementation of SHA-1 Random is substantially different from the implementation in RSA Data Security, Inc.'s Java cryptographic toolkit, Crypto-J.

# Key Info Types

---

This chapter lists the standard key information types (KIs) offered with Crypto-C. For an explanation of the key object, see “The Key Object” on page 9. A typical application supplies a key info type as the *infoType* argument to `B_SetKeyInfo`. For examples of how to use key info types with certain algorithms, see the *User’s Manual*.

The format for each entry is shown in Figure 3-1 on page 230.

**Purpose:**  
Describes the KI, what it is for, and what it does.

**Type of information this allows you to use:**  
Describes the type and format of key information you can use with the key info type.

**Format of info returned by B\_GetKeyInfo:**  
Describes the exact format that B\_GetKeyInfo returns for the key value. This is generally a "cleaned up" version of the format supplied to B\_SetKeyInfo. For example, B\_GetKeyInfo with KI\_DES8 returns the DES key with the DES key parity set.

**Format of info supplied to B\_SetKeyInfo:**  
Describes the exact format for supplying the key value to B\_SetKeyInfo.

**Can get this info type if key object already has:**  
Most keys have multiple representations for the key information. For example, you can specify an 8-byte RC2 key with KI\_8Byte or KI\_Item. This describes what type of key information a key object must already have if you want to call B\_GetKeyInfo using this key info type.

**KI\_PKCS\_RSAPrivate**

**Purpose:**  
This KI allows you to specify a private key of the RSA algorithm as defined in PKCS #1. The information consists of the modulus, exponents, two primes and the Chinese Remainder Theorem information that are explained below. See KI\_PKCS\_RSAPrivateBER for the same key info type with BER encoding.

**Type of information this allows you to use:**  
an RSA private key where all the integers are specified as in PKCS #1: modulus, public and private exponents, and Chinese Remainder Theorem information. Note that KI\_RSA\_CRT can be used for a private key that has the modulus and Chinese Remainder Theorem information but no public or private exponent.

**Format of info supplied to B\_SetKeyInfo:**  
pointer to an A\_PKCS\_RSA\_PRIVATE\_KEY structure:

```

typedef struct {
    ITEM modulus; /* modulus */
    ITEM publicExponent; /* exponent for public key */
    ITEM privateExponent; /* exponent for private key */
    ITEM prime[2]; /* prime factors */
    ITEM primeExponent[2]; /* exponents for prime factors */
    ITEM coefficient; /* CRT coefficient */
} A_PKCS_RSA_PRIVATE_KEY;

```

Each ITEM supplies an integer in canonical format, where the ITEM's data points to an unsigned byte array, most significant byte first and the ITEM's len gives its length. All leading zeros are stripped from each integer before it is copied to the key object.

**Format of info returned by B\_GetKeyInfo:**  
pointer to an A\_PKCS\_RSA\_PRIVATE\_KEY structure (see above). All leading zeros have been stripped from each integer in the structure.

**Can get this info type if key object already has:**  
KI\_PKCS\_RSAPrivate, KI\_PKCS\_RSAPrivateBER or KI\_RSA\_CRT.

Figure 3-1 Sample Key Info Type

## KI\_8Byte

### Purpose:

This KI allows you to specify a generic 8-byte key for a symmetric encryption algorithm that may be RC2, DES, or any other symmetric algorithm. For DES encryption, there exist more specific variants of 8-byte key info types: KI\_DES8 and KI\_DES8Strong.

### Type of information this allows you to use:

an 8-byte value for symmetric keys such as DES and RC2. Note that KI\_DES8Strong is usually used for a DES key because it sets the DES parity and checks for weak DES keys.

### Format of *info* supplied to B\_SetKeyInfo:

pointer to an unsigned char array that holds the 8 bytes.

### Format of *info* returned by B\_GetKeyInfo:

pointer to an unsigned char array that holds the 8 bytes.

### Can get this info type if key object already has:

KI\_8Byte, KI\_Item (if the length of the ITEM is 8), or KI\_DES8.

## KI\_24Byte

### Purpose:

This KI allows you to specify a generic 24-byte key for a symmetric encryption algorithm such as Triple DES. It may also be used as keying material for certain MAC algorithms such as HMAC. See KI\_DES24Strong for a Triple DES specific variant of this key info type.

### Type of information this allows you to use:

a 24-byte value for symmetric keys such as DES\_EDE.

### Format of *info* supplied to B\_SetKeyInfo:

pointer to an unsigned char array that holds the 24 bytes.

### Format of *info* returned by B\_GetKeyInfo:

pointer to an unsigned char array that holds the 24 bytes.

### Can get this info type if key object already has:

KI\_24Byte, KI\_Item (if the length of the ITEM is 24), KI\_DESX.

## KI\_DES8

### Purpose:

This KI allows you to specify an 8-byte key used by the DES algorithm. The key object will satisfy the DES parity requirement. Unlike `KI_DES8Strong`, it does not check against known DES weak keys. See the user manual, *DES Weak Keys*.

### Type of information this allows you to use:

an 8-byte value for a DES key where the information stored in the key object must be DES parity adjusted according to FIPS 46-1. Crypto-C treats the least significant bit of each byte of the key data as the DES parity adjustment bit.

### Format of *info* supplied to `B_SetKeyInfo`:

pointer to an unsigned char array that holds the 8-byte DES key. The key is DES parity adjusted when it is copied to the key object.

For added security, it is prudent to check the proposed key data against known byte sequences that produce weak DES keys before calling `B_SetKeyInfo`. See Section 5.6 "DES Weak Keys."

### Format of *info* returned by `B_GetKeyInfo`:

pointer to an unsigned char array that holds the 8-byte DES key that is DES parity adjusted.

### Can get this info type if key object already has:

`KI_DES8`, `KI_Item` (if the length of the `ITEM` is 8 and the data's DES parity is correct), or `KI_8Byte` (if the DES parity is correct).

### Notes:

It is more secure to use `KI_DES8Strong` instead of `KI_DES8`. When you call `B_SetAlgorithmInfo` with `KI_DES8Strong`, Crypto-C checks the key against a list of known weak keys and returns an error if the resulting key would be weak. See Section 5.6 "DES Weak Keys."

## KI\_DES8Strong

### Purpose:

This KI allows you to specify an 8-byte key used by the DES algorithm. The key object will satisfy the DES parity requirement and will be checked against known DES weak keys. Also see KI\_DES8.

### Type of information this allows you to use:

an 8-byte value for a DES key where the information stored in the key object will be DES parity adjusted according to FIPS 46-1. Crypto-C treats the least significant bit of each byte of the key data as the DES parity adjustment bit. When setting a key object with this KI, Crypto-C will check the input data against a list of known DES weak keys. If the resulting key would be weak, Crypto-C returns an error.

### Format of *info* supplied to B\_SetKeyInfo:

pointer to an unsigned char array that holds the 8-byte DES key. The key is DES parity adjusted when it is copied to the key object.

### Format of *info* returned by B\_GetKeyInfo:

pointer to an unsigned char array that holds the 8-byte DES key, which is DES parity adjusted.

### Can get this info type if key object already has:

KI\_DES8Strong, KI\_DES8 (if the key is not weak), KI\_Item (if the length of the ITEM is 8, the data's DES parity is correct, and the key is not weak), or KI\_8Byte (if the DES parity is correct and the key is not weak).

## KI\_DES24Strong

### Purpose:

This KI allows you to specify a 24-byte key used by the Triple DES algorithm. The key object will satisfy the DES parity requirement and will be checked against known DES weak keys.

### Type of information this allows you to use:

24-byte value for a Triple DES key where the information stored in the key object will be DES parity-adjusted according to FIPS 46-1. Crypto-C treats the least significant bit of each byte of the key data as the DES parity-adjustment bit. When setting a key object with this KI, Crypto-C will check the input data against a list of known DES weak keys. If the resulting key would be weak, Crypto-C returns an error.

### Format of *info* supplied to B\_SetKeyInfo:

pointer to an unsigned char array that holds the 24-byte Triple DES key. The key is DES parity adjusted when it is copied to the key object.

### Format of *info* returned by B\_GetKeyInfo:

pointer to an unsigned char array that holds the 24-byte Triple DES key that is DES parity adjusted.

### Can get this info type if key object already has:

KI\_DES24Strong, KI\_24Byte (if the key is not weak), KI\_ITEM (if the length of the ITEM is 24 and the key is not weak), KI\_DESX (if the key is not weak).

## KI\_DES\_BSAFE1

### Purpose:

Deprecated. This type is included only for backward compatibility.

### Type of information this allows you to use:

the BSAFE 1.x encoding of a DES key.

### Format of *info* supplied to B\_SetKeyInfo:

pointer to an ITEM structure that gives the address and length of the BSAFE 1.x encoding. B\_SetKeyInfo returns BE\_WRONG\_KEY\_INFO if the encoding specifies a secret key for an algorithm other than DES.

### Format of *info* returned by B\_GetKeyInfo:

pointer to an ITEM structure that gives the address and length of the BSAFE 1.x encoding.

### Can get this info type if key object already has:

KI\_DES\_BSAFE1, KI\_DES8, KI\_ITEM (if the length of the ITEM is 8 and the data's DES parity is correct), KI\_8Byte (if the DES parity is correct), KI\_RC2WithBSAFE1Params (if the DES parity of the RC2 key is correct) or KI\_RC2\_BSAFE1 (if the DES parity of the 8 Byte RC2 key is correct).

## KI\_DESX

### Purpose:

This KI allows you to specify keying materials for the DESX algorithm. They include the key value, input whitener, and output whitener. The key value will be used as the DES encryption key for the DESX algorithm and thus it will be parity adjusted. See the AI\_DESX\_CBC\_IV8 section for descriptions of the DESX algorithm.

### Type of information this allows you to use:

a DESX key where the key value, input whitener, and output whitener are specified.

### Format of *info* supplied to B\_SetKeyInfo:

pointer to an A\_DESX\_KEY structure:

```
typedef struct {
    unsigned char *key;                /* pointer to 8-byte key */
    unsigned char *inputWhitener;      /* pointer to 8-byte input whitener */
    unsigned char *outputWhitener;     /* pointer to 8-byte output whitener */
} A_DESX_KEY;
```

The value of key is DES parity adjusted when it is copied to the key object.

### Format of *info* returned by B\_GetKeyInfo:

pointer to an A\_DESX\_KEY structure (see above). The value of key is DES parity adjusted.

### Can get this info type if key object already has:

KI\_24Byte (if the DES parity is correct), KI\_Item (if the length of the ITEM is 24 and the data's DES parity is correct), or KI\_DESX.

## KI\_DESX\_BSAFE1

### Purpose:

Deprecated. This type is included only for backward compatibility.

### Type of information this allows you to use:

the BSAFE 1.x encoding of a DESX key.

### Format of *info* supplied to B\_SetKeyInfo:

pointer to an ITEM structure that gives the address and length of the BSAFE 1.x encoding. B\_SetKeyInfo returns BE\_WRONG\_KEY\_INFO if the encoding specifies a secret key for an algorithm other than DESX.

### Format of *info* returned by B\_GetKeyInfo:

pointer to an ITEM structure that gives the address and length of the BSAFE 1.x encoding.

### Can get this info type if key object already has:

KI\_DESX\_BSAFE1 or KI\_DESX (if the output whitener is the MAC of the key and the input whitener).

## KI\_DSAPrivate

### Purpose:

This KI allows you to specify a private key used by the DSA algorithm. The information consists of a private component and the three parameters:  $p$ ,  $q$ , and  $g$ , which are explained below. See `KI_DSAPrivateBER` or `KI_DSAPrivateX957BER` for the same key type with BER encoding.

### Type of information this allows you to use:

a DSA private key. The parameters of the key are specified as the following: private component ( $x$ ), the prime ( $p$ ), the subprime ( $q$ ) and the base ( $g$ ).

### Format of *info* supplied to `B_SetKeyInfo`:

pointer to an `A_DSA_PRIVATE_KEY` structure:

```
typedef struct {
    ITEM x; /* private component */
    A_DSA_PARAMS params; /* the DSA parameters, p, q and g */
} A_DSA_PRIVATE_KEY;
```

where `A_DSA_PARAMS` is defined as

```
typedef struct {
    ITEM prime; /* the prime p */
    ITEM subPrime; /* the subprime q */
    ITEM base; /* the base g */
} A_DSA_PARAMS;
```

Each `ITEM` supplies an integer in canonical format, where the `ITEM`'s data points to an unsigned byte array, most significant byte first and the `ITEM`'s len gives its length. All leading zeros are stripped from each integer before it is copied to the key object.

### Format of *info* returned by `B_GetKeyInfo`:

pointer to an `A_DSA_PRIVATE_KEY` structure (see above). All leading zeros have been stripped from each integer in the structure.

## Can get this info type if key object already has:

KI\_DSAPrivate, KI\_DSAPrivateBER, or KI\_DSAPrivateX957BER.

---

## KI\_DSAPrivateBER

### Purpose:

This KI is similar to `KI_DSAPrivate` except that it uses the ASN.1 BER format. This KI allows you to parse and create an ASN.1 key info type encoded with the PKCS #8 standard. You call `B_SetKeyInfo` to initialize a key object from the encoded key info type that includes the private component, prime, subprime, and base. You call `B_GetKeyInfo` with this KI to create an encoded key info type from a key object that was created using `KI_DSAPrivate` or `KI_DSAPrivateBER`. The OID for DSA keys, excluding the tag and length bytes, in decimal, is "43, 14, 3, 2, 12". Also see `KI_DSAPrivate` and `KI_DSAPrivateX957BER`.

### Type of information this allows you to use:

the encoding of a DSA private key that is encoded as a PKCS #8 `PrivateKeyInfo` type and that contains an RSA Data Security, Inc. `DSAPrivateKey` type. Note that this encoding contains all of the information specified by `KI_DSAPrivate`.

### Format of *info* supplied to `B_SetKeyInfo`:

pointer to an `ITEM` structure that gives the address and length of the BER encoding. The encoding is converted to DER before it is copied to the key object. `B_SetKeyInfo` returns `BE_WRONG_KEY_INFO` if the `PrivateKeyInfo` specifies a private key for an algorithm other than DSA.

### Format of *info* returned by `B_GetKeyInfo`:

pointer to an `ITEM` structure that gives the address and length of the DER encoding.

### Can get this info type if key object already has:

`KI_DSAPrivate`, `KI_DSAPrivateBER`, or `KI_DSAPrivateX957BER`.

## KI\_DSAPrivateX957BER

### Purpose:

This KI represents the same algorithm type as `KI_DSAPrivate` except that it uses the ASN.1 BER format. It allows you to parse and create an ASN.1 key info type encoded as specified by ANSI X9.57 standard. You call `B_SetKeyInfo` to initialize a key object from the encoded key info type that includes the private component, prime, subprime, and base. You call `B_GetKeyInfo` with this KI to create an encoded key info type from a key object that was created using `KI_DSAPrivate`, `KI_DSAPrivateBER`, or `KI_DSAPrivateX957BER`. The OID for DSA keys, excluding the tag and length bytes, in decimal, is "42, 134, 72, 206, 56, 4, 1". Also see `KI_DSAPrivate` and `KI_DSAPrivateBER`.

### Type of information this allows you to use:

the encoding of a DSA private key that is encoded as ANSI X9.57 `PrivateKeyInfo` type that contains an RSA Data Security, Inc. `DSAPrivateKey` type. Note that this encoding contains all of the information specified by `KI_DSAPrivate`.

### Format of info supplied to `B_SetKeyInfo`:

pointer to an `ITEM` structure that gives the address and length of the BER encoding. The encoding is converted to DER before it is copied to the key object. `B_SetKeyInfo` returns `BE_WRONG_KEY_INFO` if the `PrivateKeyInfo` specifies a private key for an algorithm other than DSA (as defined by ANSI X9.57 standard).

### Format of info returned by `B_GetKeyInfo`:

pointer to an `ITEM` structure that gives the address and length of the DER encoding.

### Can get this info type if key object already has:

`KI_DSAPrivate`, `KI_DSAPrivateBER`, or `KI_DSAPrivateX957BER`.

## KI\_DSAPublic

### Purpose:

This KI allows you to specify a public key used by the DSA algorithm. The information consists of a private component and the three parameters:  $p$ ,  $q$ , and  $g$ , which are explained below. See KI\_DSAPublicBER or KI\_DSAPublicCX957BER for the same key type with BER encoding.

### Type of information this allows you to use:

a DSA public key where all the parameters are specified as in X9.30 Part III: the public component ( $y$ ), the prime ( $p$ ), the subprime ( $q$ ), and the base ( $g$ ).

### Format of *info* supplied to B\_SetKeyInfo:

pointer to an A\_DSA\_PUBLIC\_KEY structure:

```
typedef struct {
    ITEM y; /* public component */
    A_DSA_PARAMS params; /* the DSA parameters, p, q and g */
} A_DSA_PUBLIC_KEY;
```

where A\_DSA\_PARAMS is defined as:

```
typedef struct {
    ITEM prime; /* the prime p */
    ITEM subPrime; /* the subprime q */
    ITEM base; /* the base g */
} A_DSA_PARAMS;
```

Each ITEM supplies an integer in canonical format, where the ITEM's *data* points to an unsigned byte array, most significant byte first and the ITEM's *len* gives its length. All leading zeros are stripped from each integer before it is copied to the key object.

### Format of *info* returned by B\_GetKeyInfo:

pointer to an A\_DSA\_PUBLIC\_KEY structure (see above). All leading zeros have been stripped from each integer in the structure.

## Can get this info type if key object already has:

KI\_DSAPublic, KI\_DSAPublicBER, KI\_DSAPublicX957BER.

---

## KI\_DSAPublicBER

### Purpose:

This KI is similar to `KI_DSAPublic` except that it uses the ASN.1 BER format. This KI allows you to parse and create an ASN.1 key info type encoded with the X.509 standard for `SubjectPublicKeyInfo`. You call `B_SetKeyInfo` to initialize a key object from the encoded key info type that includes the public component, prime, subprime, and base. You call `B_GetKeyInfo` with this KI to create an encoded key info type from a key object that was created using `KI_DSAPublic` or `KI_DSAPublicBER`. The OID for DSA keys, excluding the tag and length bytes, in decimal, is "43, 14, 3, 2, 12". Also see `KI_DSAPublic` and `KI_DSAPublicX957BER`.

### Type of information this allows you to use:

the encoding of a DSA public key that is encoded as an X.509 `SubjectPublicKeyInfo` type as defined in X9.30 Part III. Note that this encoding contains all of the information specified by `KI_DSAPublic`.

### Format of *info* supplied to `B_SetKeyInfo`:

pointer to an `ITEM` structure that gives the address and length of the BER encoding. The encoding is converted to DER before it is copied to the key object. `B_SetKeyInfo` returns `BE_WRONG_KEY_INFO` if the `PublicKeyInfo` specifies a public key for an algorithm other than DSA.

### Format of *info* returned by `B_GetKeyInfo`:

pointer to an `ITEM` structure that gives the address and length of the DER encoding.

### Can get this info type if key object already has:

`KI_DSAPublic`, `KI_DSAPublicBER`, `KI_DSAPublicX957BER`.

## KI\_DSAPublicX957BER

### Purpose:

This KI is similar to `KI_DSAPublic` except that it uses the ASN.1 BER format. This KI allows you to parse and create an ASN.1 key info type encoded as specified by ANSI X9.57 standard. You call `B_SetKeyInfo` to initialize a key object from the encoded key info type that includes the public component, prime, subprime, and base. You call `B_GetKeyInfo` with this KI to create an encoded key info type from a key object that was created using `KI_DSAPublic`, `KI_DSAPublicBER`, or `KI_DSAPublicX957BER`. The OID for DSA keys, excluding the tag and length bytes, in decimal, is "42, 134, 72, 206, 56, 4, 1". Also see `KI_DSAPublic` and `KI_DSAPublicBER`.

### Type of information this allows you to use:

the encoding of a DSA public key that is encoded as ANSI X9.57 `SubjectPublicKeyInfo` type. Note that this encoding contains all of the information specified by `KI_DSAPublic`.

### Format of *info* supplied to `B_SetKeyInfo`:

pointer to an `ITEM` structure that gives the address and length of the BER encoding. The encoding is converted to DER before it is copied to the key object. `B_SetKeyInfo` returns `BE_WRONG_KEY_INFO` if the `PublicKeyInfo` specifies a public key for an algorithm other than DSA (as defined by ANSI X9.57 standard).

### Format of *info* returned by `B_GetKeyInfo`:

pointer to an `ITEM` structure that gives the address and length of the DER encoding.

### Can get this info type if key object already has:

`KI_DSAPublic`, `KI_DSAPublicBER`, `KI_DSAPublicX957BER`.

## KI\_ECPrivate

### Purpose:

This KI allows you to specify a private key used by the Elliptic Curve algorithm. The information consists of the private component and the underlying elliptic curve parameters.

### Type of information this allows you to use:

an elliptic curve private key. The parameters of the key are specified as the private component *privateKey*, and the underlying elliptic curve parameters.

### Format of *info* supplied to B\_SetKeyInfo:

pointer to an A\_EC\_PRIVATE\_KEY structure:

```
typedef struct {
    A_EC_PARAMS curveParams;    /*the underlying elliptic curve parameters */
    ITEM      privateKey;        /* private component */
} A_EC_PRIVATE_KEY;
```

Each ITEM supplies an integer in canonical format, where the ITEM's *data* points to an unsigned byte array, most significant byte first, and the ITEM's *len* gives its length. For all ITEM values except the curve parameter base, leading zeros are stripped before it is copied to the key object.

### Format of *info* returned by B\_GetKeyInfo:

pointer to an A\_EC\_PRIVATE\_KEY structure.

### Can get this info type if key object already has:

KI\_ECPrivate.

## KI\_ECPrivateComponent

### Purpose:

This KI allows you to specify the private component of an EC private key. Unlike KI\_ECPrivate, it does not contain the underlying EC parameters and it is not to be used with any algorithms. It provides a way to extract the EC private key.

### Type of information this allows you to use:

the private component of an EC private key.

### Format of *info* supplied to B\_SetKeyInfo:

pointer to an ITEM structure containing the private component of an EC private key.

### Format of *info* returned by B\_GetKeyInfo:

pointer to an ITEM structure containing the private component of an EC private key.

### Restrictions:

Key objects built with this KI are not compatible with any Crypto-C AI. This KI is supplied only as a convenience to extract the EC private component.

### Can get this info type if key object already has:

KI\_ECPrivateComponent or KI\_ECPrivate.

## KI\_ECPublic

### Purpose:

This KI allows you to specify a public key used by the Elliptic Curve algorithm. The information consists of the public component and the underlying elliptic curve parameters.

### Type of information this allows you to use:

an elliptic curve public key. The parameters of the key are specified as the public component (*publicKey*), and the underlying elliptic curve parameters.

### Format of *info* supplied to B\_SetKeyInfo:

pointer to an A\_EC\_PUBLIC\_KEY structure:

```
typedef struct {
    A_EC_PARAMS curveParams;    /*the underlying elliptic curve parameters */
    ITEM        publicKey;      /* public component */
} A_EC_PUBLIC_KEY;
```

Each ITEM supplies an integer in canonical format, where the ITEM's data points to an unsigned byte array, most significant byte first, and the ITEM's len gives its length. For all ITEM values except the public component (x) and the curve parameter base, leading zeros are stripped before it is copied to the key object.

### Format of *info* returned by B\_GetKeyInfo:

pointer to an A\_EC\_PUBLIC\_KEY structure.

### Can get this info type if key object already has:

KI\_ECPublic.

## KI\_ECPublicComponent

### Purpose:

This KI allows you to specify the public key component of an EC public key. Unlike `KI_ECPublic`, it does not specify the underlying EC parameters and it is not to be used with any algorithms. It provides a way to extract the EC public key.

### Type of information this allows you to use:

the public component of an elliptic curve public key.

### Format of *info* supplied to `B_SetKeyInfo`:

pointer to an `ITEM` structure containing the public component of an EC public key.

### Format of *info* returned by `B_GetKeyInfo`:

pointer to an `ITEM` structure containing the public component of an EC public key.

### Restrictions:

Key objects built with this KI are not compatible with any Crypto-C AI. This KI is supplied only as a convenience to extract the EC public component.

### Can get this info type if key object already has:

`KI_ECPublicComponent` or `KI_ECPublic`.

## KI\_ExtendedToken



### Purpose:

This KI allows you to specify a software-based token form of a symmetric key. See KI\_KeypairToken for a token form of a public/private key pair.

### Type of information this allows you to use:

software-based token forms of symmetric keys. Downward compatible with KI-Token.

### Format of *info* supplied to B\_SetKeyInfo:

pointer to a KI\_EXTENDED\_TOKEN\_INFO structure

```
typedef struct {
    KI_TOKEN_INFO      keyDataStruct;
    A_X509_ATTRIB_INFO attributes;
} KI_EXTENDED_TOKEN_INFO;
```

where A\_X509\_ATTRIB\_INFO is defined by:

```
typedef struct {
    A_SYMMETRIC_KEY_DEFINER external Specs;
    unsigned char           *keyOID,           /* Currently unimplemented */
    unsigned int            keyOIDLen,         /* ditto */
    unsigned long           dateOfBirth,       /* When the key was created. */
    /* This time stamp currently defaults to time () function */
} A_X509_ATTRIB_INFO;
```

and A\_SYMMETRIC\_KEY\_DEFINER is defined by:

```
typedef struct {
    unsigned int keyUsage;
    unsigned int keyLengthInBytes;
    UINT4       lifeTime;
    unsigned int protectFlag;
} A_SYMMETRIC_KEY_DEFINER;
```

### Format of *info* returned by B\_GetKeyInfo:

pointer to a KI\_EXTENDED\_TOKEN\_INFO structure (see above).

### Can get this info type if key object already has:

a symmetric key of the appropriate type, for example, a DES key when using DES. Used when one of the algorithm methods used by AI\_SymKeyTokenGen has been listed in the *fixedChooser* argument to B\_CreateSessionChooser, but no hardware is present.

### Notes:

KI\_ExtendedToken can only be used if you have called B\_CreateSessionChooser for your application.

---

## KI\_Item

### Purpose:

This KI allows you to specify a generic keying material of any length. It may be used to hold a secret key of a symmetric encryption algorithm, a key of a keyed hash algorithm, a password object, etc.

### Type of information this allows you to use:

a variable-length block of data (such as an RC4 key), a password for password-based encryption algorithms, or the value of a secret key when it is recovered from a public-key encryption block.

### Format of *info* supplied to B\_SetKeyInfo:

pointer to an ITEM structure:

```
typedef struct {
    unsigned char *data;
    unsigned int   len;
} ITEM;
```

where *data* is the address of the unsigned byte array and *len* is its length.

### Format of *info* returned by B\_GetKeyInfo:

pointer to an ITEM structure (see above)

### Can get this info type if key object already has:

KI\_Item, KI\_8Byte, KI\_24Byte, KI\_DES8, KI\_DES8Strong, or KI\_DESX.

# KI\_KeypairToken



## Purpose:

This KI allows you to specify the software-based token form of a public and private key pair of type RSA or DSA. See KI\_ExtendedToken for the token form of a symmetric key.

## Type of information this allows you to use:

software-based token forms of RSA or DSA public and private key pairs. Downward compatible with KI-Token.

## Format of *info* supplied to B\_SetKeyInfo:

pointer to a KI\_KEYPAIR\_TOKEN\_INFO structure:

```
typedef struct {
    KI_TOKEN_INFO          keyDataStruct;
    A_X509_KEYPAIR_ATTRIB_INFO attributes;
} KI_KEYPAIR_TOKEN_INFO;
```

where A\_X509\_KEYPAIR\_ATTRIB\_INFO is defined by:

```
typedef struct {
    A_KEYPAIR_DEFINDER external Specs;
    unsigned long      dateOfBirth;
} A_X509_KEYPAIR_ATTRIB_INFO;
```

and A\_KEYPAIR\_DEFINDER is defined by:

```
typedef struct {
    unsigned int keyUsage;          /* X509 key usage bit map */
    UINT4       lifetime;          /* Key lifetime; under consideration */
    unsigned int protectFlag;      /* Store key in encrypted form */
} A_KEYPAIR_DEFINDER;
```

## Format of *info* returned by B\_GetKeyInfo:

pointer to a KI\_KEYPAIR\_TOKEN\_INFO structure.

## Can get this info type if key object already has:

an RSA or DSA key pair. Used when one of the algorithm methods used by `KI_KeypairTokenGen` has been listed in the *fixedChooser* argument to `B_CreateSessionChooser`, but no hardware is present.

## Notes:

`KI_KeypairToken` can only be used if you have called `B_CreateSessionChooser` for your application.

## KI\_PKCS\_RSAPrivate

### Purpose:

This KI allows you to specify a private key of the RSA algorithm as defined in PKCS #1. The information consists of the modulus, exponents, two primes, and the Chinese Remainder Theorem information. See KI\_PKCS\_RSAPrivateBER for the same key info type with BER encoding.

### Type of information this allows you to use:

an RSA private key where all the integers are specified as in PKCS #1: modulus, public and private exponents, and Chinese Remainder Theorem information. Note that KI\_RSA\_CRT can be used for a private key that has the modulus and Chinese Remainder Theorem information but no public or private exponent.

### Format of *info* supplied to B\_SetKeyInfo:

pointer to an A\_PKCS\_RSA\_PRIVATE\_KEY structure:

```
typedef struct {
    ITEM modulus; /* modulus */
    ITEM publicExponent; /* exponent for public key */
    ITEM privateExponent; /* exponent for private key */
    ITEM prime[2]; /* prime factors */
    ITEM primeExponent[2]; /* exponents for prime factors */
    ITEM coefficient; /* CRT coefficient */
} A_PKCS_RSA_PRIVATE_KEY;
```

Each ITEM supplies an integer in canonical format, where the ITEM's *data* points to an unsigned byte array, most significant byte first and the ITEM's *len* gives its length. All leading zeros are stripped from each integer before it is copied to the key object.

### Format of *info* returned by B\_GetKeyInfo:

pointer to an A\_PKCS\_RSA\_PRIVATE\_KEY structure (see above). All leading zeros have been stripped from each integer in the structure.

### Can get this info type if key object already has:

KI\_PKCS\_RSAPrivate, KI\_PKCS\_RSAPrivateBER, or KI\_RSA\_CRT.

---

## KI\_PKCS\_RSAPrivateBER

### Purpose:

This KI is similar to `KI_PKCS_RSAPrivate` except that it uses the ASN.1 BER format. This KI allows you to parse and create an ASN.1 key info type that is encoded with the PKCS #8 standard. You call `B_SetKeyInfo` to initialize a key object from the encoded key info type that includes the modulus, exponents, two primes, and Chinese Remainder Theorem information. You call `B_GetKeyInfo` with this KI to create an encoded key info type from a key object that was created using `KI_PKCS_RSAPrivate`, `KI_PKCS_RSAPrivateBER` or `KI_RSA_CRT`. The OID for RSA PKCS #1 encryption, excluding the tag and length bytes, in decimal, is "42, 134, 72, 134, 247, 13, 1, 1, 1". Also see `KI_PKCS_RSAPrivate`.

### Type of information this allows you to use:

the encoding of an RSA private key that is encoded as a PKCS #8 `PrivateKeyInfo` type that contains a PKCS #1 `RSAPrivateKey` type. Note that this encoding contains all of the information specified by `KI_PKCS_RSAPrivate`.

### Format of *info* supplied to `B_SetKeyInfo`:

pointer to an `ITEM` structure that gives the address and length of the BER encoding. The encoding is converted to DER before it is copied to the key object. `B_SetKeyInfo` returns `BE_WRONG_KEY_INFO` if the *PrivateKeyInfo* specifies a private key for an algorithm other than RSA.

### Format of *info* returned by `B_GetKeyInfo`:

pointer to an `ITEM` structure that gives the address and length of the DER encoding.

### Can get this info type if key object already has:

`KI_PKCS_RSAPrivate`, `KI_PKCS_RSAPrivateBER` or `KI_RSA_CRT`.

## KI\_RC2\_BSAFE1

### Purpose:

Deprecated. This type is included only for backward compatibility.

### Type of information this allows you to use:

the BSAFE 1.x encoding of an RC2 key, which is the same as an SX1 key.

### Format of *info* supplied to B\_SetKeyInfo:

pointer to an ITEM structure that gives the address and length of the BSAFE 1.x encoding. B\_SetKeyInfo returns BE\_WRONG\_KEY\_INFO if the encoding specifies a secret key for an algorithm other than RC2 (which is the same as SX1).

### Format of *info* returned by B\_GetKeyInfo:

pointer to an ITEM structure that gives the address and length of the BSAFE 1.x encoding.

### Can get this info type if key object already has:

KI\_RC2\_BSAFE1 or KI\_RC2WithBSAFE1Params.

## KI\_RC2WithBSAFE1Params

### Purpose:

Deprecated. This type is included only for backward compatibility.

### Type of information this allows you to use:

an RC2 key (which is the same as an SX1 key) where the key value and effective key size are specified. Usually, the effective key size is a parameter to the RC2 encryption algorithm; however, BSAFE 1.x also encodes the effective key size with the RC2 key.

### Format of *info* supplied to B\_SetKeyInfo:

pointer to a B\_RC2\_BSAFE1\_PARAMS\_KEY structure:

```
typedef struct {
    unsigned char *key;                /* pointer to 8-byte key */
    unsigned int  effectiveKeyBits;    /* effective key size parameter */
} B_RC2_BSAFE1_PARAMS_KEY;
```

*effectiveKeyBits* must be between 2 and 64, inclusive. The value of *key* is adjusted when it is copied to the key object by zeroizing unneeded bytes because *effectiveKeyBits* is smaller than 64. For example, if *effectiveKeyBits* is 32 and the hexadecimal value of *key* is 0102030405060708, then 0102030400000000 is copied to the key object because only 32 bits (4 bytes) are needed.

### Format of *info* returned by B\_GetKeyInfo:

pointer to a B\_RC2\_BSAFE1\_PARAMS\_KEY structure (see above). The value of *key* is adjusted by zeroizing unneeded bytes based on the *effectiveKeyBits* as explained above.

### Can get this info type if key object already has:

KI\_RC2WithBSAFE1Params or KI\_RC2\_BSAFE1.

## KI\_RSA\_CRT

### Purpose:

This KI allows you to specify a private key of the RSA algorithm without the public or private key exponent information. The modulus and Chinese Remainder Theorem information have to be provided.

### Type of information this allows you to use:

an RSA private key where the modulus and Chinese Remainder Theorem information integers are specified, but not the public or private exponent integers. (For RSA private key information with the public and private exponent integers, see KI\_PKCS\_RSAPrivate.)

### Format of *info* supplied to B\_SetKeyInfo:

pointer to an A\_RSA\_CRT\_KEY structure:

```
typedef struct {
    ITEM modulus; /* modulus */
    ITEM prime[2]; /* prime factors */
    ITEM primeExponent[2]; /* exponents for prime factors */
    ITEM coefficient; /* CRT coefficient */
} A_RSA_CRT_KEY;
```

Each ITEM supplies an integer in canonical format, where the ITEM's *data* points to an unsigned byte array, most significant byte first and the ITEM's *len* gives its length. All leading zeros are stripped from each integer before it is copied to the key object.

### Format of *info* returned by B\_GetKeyInfo:

pointer to an A\_RSA\_CRT\_KEY structure (see above). All leading zeros have been stripped from each integer in the structure.

### Can get this info type if key object already has:

KI\_RSA\_CRT, KI\_PKCS\_RSAPrivate, or KI\_PKCS\_RSAPrivateBER.

## KI\_RSAPrivate

### Purpose:

This KI allows you to specify an RSA private key with the modulus and private key exponent. Unlike KI\_PKCS\_RSAPrivate, it does not contain the Chinese Remainder Theorem information and it is not be used with any algorithms. It provides a way to store or transport a private key.

### Type of information this allows you to use:

an RSA private key where the modulus and private exponent integers are specified, but not the Chinese Remainder Theorem information.

### Format of *info* supplied to B\_SetKeyInfo:

pointer to an A\_RSA\_KEY structure:

```
typedef struct {
    ITEM modulus;           /* modulus */
    ITEM exponent;        /* exponent */
} A_RSA_KEY;
```

Each ITEM supplies an integer in canonical format, where the ITEM's *data* points to an unsigned byte array, most significant byte first and the ITEM's *len* gives its length. All leading zeros are stripped from each integer before it is copied to the key object.

### Format of *info* returned by B\_GetKeyInfo:

pointer to an A\_RSA\_KEY structure (see above). All leading zeros have been stripped from each integer in the structure.

### Can get this info type if key object already has:

KI\_RSAPrivate, KI\_PKCS\_RSAPrivate or KI\_PKCS\_RSAPrivateBER.

### Note:

You can use KI\_RSAPrivate to set a key object with your private modulus and private exponent. This can be used for storing your key information or when you need to export the information in “raw” form to another application. However, there are no

---

KL\_RSAPrivate

---

Crypto-C algorithms that use this key type.

## KI\_RSAPrivateBSAFE1

### Purpose:

Deprecated. This type is included only for backward compatibility.

### Type of information this allows you to use:

the BSAFE 1.x encoding of an RSA private key.

### Format of *info* supplied to B\_SetKeyInfo:

pointer to an ITEM structure that gives the address and length of the BSAFE 1.x encoding. B\_SetKeyInfo returns BE\_WRONG\_KEY\_INFO if the encoding specifies a private key for an algorithm other than RSA.

### Format of *info* returned by B\_GetKeyInfo:

pointer to an ITEM structure that gives the address and length of the BSAFE 1.x encoding.

### Can get this info type if key object already has:

KI\_RSAPrivateBSAFE1, KI\_RSA\_CRT, KI\_PKCS\_RSAPrivate or KI\_PKCS\_RSAPrivateBER.

## KI\_RSAPublic

### Purpose:

This KI allows you to specify an RSA public key with the modulus and public key exponent. See KI\_RSAPublicBER for the same key info type with BER encoding.

### Type of information this allows you to use:

an RSA public key where the modulus and exponent integers are specified.

### Format of *info* supplied to B\_SetKeyInfo:

pointer to an A\_RSA\_KEY structure:

```
typedef struct {  
    ITEM modulus;                /* modulus */  
    ITEM exponent;              /* exponent */  
} A_RSA_KEY;
```

Each ITEM supplies an integer in canonical format, where the ITEM's *data* points to an unsigned byte array, most significant byte first and the ITEM's *len* gives its length. All leading zeros are stripped from each integer before it is copied to the key object.

### Format of *info* returned by B\_GetKeyInfo:

pointer to an A\_RSA\_KEY structure (see above). All leading zeros have been stripped from each integer in the structure.

### Can get this info type if key object already has:

KI\_RSAPublic, KI\_RSAPublicBER, KI\_PKCS\_RSAPrivate, or KI\_PKCS\_RSAPrivateBER.

---

## KI\_RSAPublicBER

### Purpose:

This KI is similar to `KI_RSAPublic` except that it uses the ASN.1 BER format. This KI allows you to parse and create an ASN.1 key info type that is encoded with the X.509 standard of `SubjectPublicKeyInfo`. You call `B_SetKeyInfo` to initialize a key object from the encoded key info type that includes the modulus and public exponent. You call `B_GetKeyInfo` with this KI to create an encoded key info type from a key object that was created using `KI_RSAPublic`, `KI_RSAPublicBER`, `KI_PKCS_RSAPrivate` or `KI_PKCS_RSAPrivateBER`. The OID for RSA PKCS #1 encryption, excluding the tag and length bytes, in decimal, is "42, 134, 72, 134, 247, 13, 1, 1, 1". Also see `KI_RSAPublic`.

### Type of information this allows you to use:

the encoding of an RSA public key that is encoded as an X.509 `SubjectPublicKeyInfo` type that contains an X.509 `RSAPublicKey` type (also defined in PKCS #1). Note that this encoding contains all of the information specified by `KI_RSAPublic`.

### Format of *info* supplied to `B_SetKeyInfo`:

pointer to an `ITEM` structure that gives the address and length of the BER encoding. The encoding is converted to DER before it is copied to the key object. `B_SetKeyInfo` returns `BE_WRONG_KEY_INFO` if the public key info specifies a public key for an algorithm other than RSA. Note that `B_SetKeyInfo` will accept an encoding that contains an object identifier for `rsa` as well as `rsaEncryption` (defined in PKCS #1).

### Format of *info* returned by `B_GetKeyInfo`:

pointer to an `ITEM` structure that gives the address and length of the DER encoding. Note that `B_GetKeyInfo` returns an encoding that contains the object identifier for `rsaEncryption` (defined in PKCS #1) as opposed to `rsa`.

### Can get this info type if key object already has:

`KI_RSAPublicBER`, `KI_RSAPublic`, `KI_PKCS_RSAPrivate`, or `KI_PKCS_RSAPrivateBER`.

## KI\_RSAPublicBSAFE1

### Purpose:

Deprecated. This type is included only for backward compatibility.

### Type of information this allows you to use:

the BSAFE 1.x encoding of an RSA public key.

### Format of *info* supplied to B\_SetKeyInfo:

pointer to an ITEM structure that gives the address and length of the BSAFE 1.x encoding. B\_SetKeyInfo returns BE\_WRONG\_KEY\_INFO if the encoding specifies a public key for an algorithm other than RSA.

### Format of *info* returned by B\_GetKeyInfo:

pointer to an ITEM structure that gives the address and length of the BSAFE 1.x encoding.

### Can get this info type if key object already has:

KI\_RSAPublicBSAFE1, KI\_RSAPublic, KI\_PKCS\_RSAPrivate, KI\_PKCS\_RSAPrivateBER or KI\_RSAPublicBER.

## KI\_Token



### Purpose:

This KI allows you to specify a hardware-based token form of a key, which may be either a symmetric key or a public/private key pair. Also see KI\_ExtendedToken and KI\_KeypairToken for other key info types with token forms.

### Type of information this allows you to use:

hardware-based token forms of symmetric keys and public/private key pairs.

### Format of *info* supplied to B\_SetKeyInfo:

pointer to a KI\_TOKEN\_INFO structure:

```
typedef struct {
    ITEM manufacturerId;           /* tag used to differentiate */
                                   /* different hardware tokens */
    ITEM internalKey;             /* OEM-supplied key handle */
} KI_TOKEN_INFO;
```

### Format of *info* returned by B\_GetKeyInfo:

pointer to a KI\_TOKEN\_INFO structure (see above).

### Can get this info type if key object already has:

a key object of the appropriate type, for example, an RSA key pair for RSA or a DES key for DES. Hardware that uses key tokens must be present.

### Notes:

Can only be used in conjunction with a hardware implementation; in particular, KI\_Token can only be used if you have called B\_CreateSessionChooser for your application.

---

KL-Token

---

# Details of Crypto-C Functions

---

This section describes the toolkit's top level API and its bottom level platform-specific routines. The procedures with names that start "B\_" make up the top level API which is called by applications. The procedure names starting with "T\_" are called by the toolkit's internal routines to perform platform-specific operations like allocating and copying memory.

## B\_BuildTableFinal

```
int B_BuildTableFinal (  
    B_ALGORITHM_OBJ buildTableObj,           /* table-building object */  
    unsigned char *accelTable,              /* acceleration table buffer */  
    unsigned int *accTableByteLen,          /* size of */  
                                           /* created acceleration table in bytes */  
    unsigned int maxAccTableLength,         /* size of */  
                                           /* acceleration table buffer */  
    A_SURRENDER_CTX *surrenderCtx         /* surrender context */  
);
```

### Description

Generates and outputs the acceleration table to *accelTable*, setting *accTableByteLen* to the number of bytes output. It returns BE\_OUTPUT\_LEN if *maxAccTableLength* is smaller than needed.

### Return value

---

Value	Description
0	Operation was successful.
non-zero	Error. See Appendix A, "Crypto-C Error Types."

---

---

## B\_BuildTableGetBufSize

```
int B_BuildTableGetBufSize (  
    B_ALGORITHM_OBJ buildTableObj,           /* table-building object */  
    unsigned int    *tableSizeInBytes       /* size of table in bytes */  
);
```

### Description

Sets *tableSizeInBytes* to the buffer size needed to accommodate the generated table.

### Return value

---

Value	Description
0	Operation was successful.
non-zero	see Appendix A, "Crypto-C Error Types"

---

## B\_BuildTableInit

```
int B_BuildTableInit (  
    B_ALGORITHM_OBJ buildTableObj,          /* table-building object */  
    B_ALGORITHM_CHOOSER algorithmChooser,  /* algorithm chooser */  
    A_SURRENDER_CTX surrenderCtx          /* surrender context */  
);
```

### Description

Initializes a table-building object used to build acceleration tables for elliptic curve cryptography.

### Return value

---

Value	Description
0	Operation was successful.
non-zero	see Appendix A, "Crypto-C Error Types"

---

## B\_CreateAlgorithmObject

```
int B_CreateAlgorithmObject (  
    B_ALGORITHM_OBJ *algorithmObject           /* new algorithm object */  
);
```

### Description

`B_CreateAlgorithmObject` allocates and initializes a new algorithm object, storing the result in `algorithmObject`. If `B_CreateAlgorithmObject` is unsuccessful, no memory is allocated and `algorithmObject` is set to `(B_ALGORITHM_OBJ)NULL_PTR`.

### Return value

---

Value	Description
0	Operation was successful.
non-zero	see Appendix A, "Crypto-C Error Types"

---

## B\_CreateKeyObject

```
int B_CreateKeyObject (  
    B_KEY_OBJ *keyObject                                /* new key object */  
);
```

### Description

`B_CreateKeyObject` allocates and initializes a new key object, storing the result in `keyObject`. If `B_CreateKeyObject` is unsuccessful, no memory is allocated and `keyObject` is set to `(B_KEY_OBJ)NULL_PTR`.

### Return value

---

Value	Description
0	Operation was successful.
non-zero	see Appendix A, "Crypto-C Error Types"

---

## B\_CreateSessionChooser



```

int B_CreateSessionChooser (
    B_ALGORITHM_CHOOSER fixedChooser,           /* Chooser consisting of */
                                                /* software-based algorithm methods. */
    B_ALGORITHM_CHOOSER *sessionChooser,       /* Runtime chooser */
                                                /* dynamically bound to available hardware based methods. */

    HW_TABLE_ENTRY      *staticHardwareList [ ], /* List of statically defined */
                                                /* hardware methods terminated by a */
                                                /* properly cast NULL_PTR. */
    ITEM                *passPhrase,           /* hardware passphrase */
    POINTER              *amTagList,          /* For now pass (*)NULL_PTR */
    unsigned char       ***listOfOEMTags,     /* Returns list of OEM tags */
                                                /* for methods in sessionChooser */
);

```

### Description

B\_CreateSessionChooser replicates the fixed chooser inclusive of making private copies of the AM structures. Whenever possible the software-based methods are replaced with the hardware-based methods defined either statically by *staticHardwareList* or dynamically determined by platform specific routines. All methods in the *fixedChooser* will be represented in the *sessionChooser* and will appear multiple times if there are multiple hardware substitutes available.

### Notes:

It is a simple matter to limit the binding of hardware methods to exclusively static or dynamically defined entries. The algorithm method structures that constitute *sessionChooser* are B\_METHOD structures extended to include an information pointer and a finalization function to destroy it.

### Return value

Value	Description
0	Operation was successful.
nonzero	unsuccessful, allocation error

## B\_DecodeDigestInfo

```
int B_DecodeDigestInfo (  
    ITEM          *algorithmID,          /* message digest algorithm identifier */  
    ITEM          *digest,                /* message digest value */  
    unsigned char *digestInfo,          /* digestInfo encoding */  
    unsigned int  digestInfoLen         /* length of digestInfo */  
);
```

### Description

`B_DecodeDigestInfo` decodes the BER encoding of a PKCS #1 `DigestInfo` type that is given by *digestInfo* of length *digestInfoLen*. On output, the *algorithmID* ITEM gives the digest algorithm identifier and the *digest* ITEM gives the digest value. The ITEM type is defined by the `KI_Item` key info type in Chapter 3.

### Return value

---

Value	Description
0	Operation was successful.
non-zero	see Appendix A, "Crypto-C Error Types"

---

## B\_DecodeFinal

```
int B_DecodeFinal (
    B_ALGORITHM_OBJ algorithmObject,           /* algorithm object */
    unsigned char *partOut,                    /* output data buffer */
    unsigned int *partOutLen,                  /* length of output data */
    unsigned int maxPartOutLen                /* size of output data buffer */
);
```

### Description

`B_DecodeFinal` finalizes the decoding process specified by *algorithmObject*, writing any remaining decoded output to *partOut*, which is a buffer supplied by the caller of at least *maxPartOutLen* bytes, and setting *partOutLen* to the number of bytes written to *partOut*. *algorithmObject* is reset to the state it was in after the call to `B_DecodeInit`, so that another decoding process may be performed. See `B_DecodeInit`.

### Return value

Value	Description
0	Operation was successful.
non-zero	see Appendix A, "Crypto-C Error Types"

## B\_DecodeInit

```
int B_DecodeInit (  
    B_ALGORITHM_OBJ algorithmObject           /* algorithm object */  
);
```

### Description

`B_DecodeInit` allocates and initializes `algorithmObject` for decoding (not decrypting) data using the algorithm specified by a previous call to `B_SetAlgorithmInfo`. For example, the `AI_RFC1113Recode` algorithm provides Base64 encoding and decoding to convert binary data to and from a printable form suitable for most email systems. Notice that there are no cryptographic keys for encoding or decoding.

`B_DecodeInit` only needs to be called once to set up a decode algorithm. The `B_DecodeUpdate` routine can be called multiple times to process blocks of data, and `B_DecodeFinal` is called once to process the last block which includes removing any trailing pad bytes. After `B_DecodeFinal` is called, `B_DecodeUpdate` can be called to start decoding another sequence of blocks. There is no need to call `B_DecodeInit` again.

### Return value

---

Value	Description
0	Operation was successful.
non-zero	see Appendix A, "Crypto-C Error Types"

---

## B\_DecodeUpdate

```

int B_DecodeUpdate (
    B_ALGORITHM_OBJ algorithmObject,          /* algorithm object */
    unsigned char *partOut,                   /* output data buffer */
    unsigned int *partOutLen,                 /* length of output data */
    unsigned int maxPartOutLen,              /* size of output data buffer */
    unsigned char *partIn,                   /* input data */
    unsigned int partInLen,                  /* length of output data */
);

```

### Description

B\_DecodeUpdate updates the decoding process specified by *algorithmObject* with *partInLen* bytes from *partIn*, writing the decoded output to *partOut*, which is a buffer supplied by the caller of at least *maxPartOutLen* bytes, and setting *partOutLen* to the number of bytes written to *partOut*. B\_DecodeUpdate may be called zero or more times to supply the data by parts. See B\_DecodeInit.

### Return value

Value	Description
0	Operation was successful.
non-zero	see Appendix A, "Crypto-C Error Types"

## B\_DecryptFinal

```
int B_DecryptFinal (  
    B_ALGORITHM_OBJ algorithmObject,           /* algorithm object */  
    unsigned char *partOut,                   /* output data buffer */  
    unsigned int *partOutLen,                 /* length of output data */  
    unsigned int maxPartOutLen,              /* size of output data buffer */  
    B_ALGORITHM_OBJ randomAlgorithm,         /* random byte source */  
    A_SURRENDER_CTX *surrenderContext       /* surrender context */  
);
```

### Description

`B_DecryptFinal` finalizes the decrypting process specified by *algorithmObject*, writing any remaining decrypted output to *partOut*, which is a buffer supplied by the caller of at least *maxPartOutLen* bytes, and setting *partOutLen* to the number of bytes written to *partOut*. The algorithm object for supplying random numbers is *randomAlgorithm*; it may be `(B_ALGORITHM_OBJ) NULL_PTR` for decrypting algorithms that do not need random numbers. The surrender context for processing and canceling during lengthy operations is *surrenderContext*; if its value is `(A_SURRENDER_CTX *) NULL_PTR`, Crypto-C does not use it. *algorithmObject* is reset to the state it was in after the call to `B_DecryptInit`, so that another decrypting process may be performed. See `B_DecryptInit`.

### Return value

---

Value	Description
0	Operation was successful.
non-zero	see Appendix A, "Crypto-C Error Types"

---

## B\_DecryptInit

```
int B_DecryptInit (
    B_ALGORITHM_OBJ      algorithmObject,      /* algorithm object */
    B_KEY_OBJ            keyObject,           /* key object */
    B_ALGORITHM_CHOOSER algorithmChooser,     /* algorithm chooser */
    A_SURRENDER_CTX     *surrenderContext      /* surrender context */
);
```

### Description

`B_DecryptInit` initializes `algorithmObject` for decrypting data using the algorithm specified by a previous call to `B_SetAlgorithmInfo`. The key object for supplying the key information is `keyObject`. The chooser for selecting the algorithm method is `algorithmChooser`. The surrender context for processing and canceling during lengthy operations is `surrenderContext`; if its value is `(A_SURRENDER_CTX *)NULL_PTR`, Crypto-C does not use it.

`B_DecryptInit` only needs to be called once to set up a key. The `B_DecryptUpdate` routine can be called multiple times to process blocks of data, and `B_DecryptFinal` is called once to process the last block, which includes removing the trailing pad bytes. After `B_DecryptFinal` is called, `B_DecryptUpdate` can be called to start processing another sequence of blocks that were encrypted in the same key. If a different CBC Initialization Vector (IVs) is used with each sequence of blocks, `B_SetAlgorithmInfo` can be called with `AI_CBC_IV8` to set the new IV before calling `B_DecryptUpdate`. There is no need to call `B_DecryptInit` again with the same key.

### Return value

Value	Description
0	Operation was successful.
non-zero	see Appendix A, "Crypto-C Error Types"

## B\_DecryptUpdate

```
int B_DecryptUpdate (
    B_ALGORITHM_OBJ algorithmObject,           /* algorithm object */
    unsigned char *partOut,                    /* output data buffer */
    unsigned int *partOutLen,                  /* length of output data */
    unsigned int maxPartOutLen,                /* size of output data buffer */
    unsigned char *partIn,                    /* input data */
    unsigned int partInLen,                    /* length of input data */
    B_ALGORITHM_OBJ randomAlgorithm,          /* random byte source */
    A_SURRENDER_CTX *surrenderContext         /* surrender context */
);
```

### Description

B\_DecryptUpdate updates the decrypting process specified by *algorithmObject* with *partInLen* bytes from *partIn*, writing the decrypted output to *partOut*, which is a buffer supplied by the caller of at least *maxPartOutLen* bytes, and setting *partOutLen* to the number of bytes written to *partOut*. The algorithm object for supplying random numbers is *randomAlgorithm*; it may be (B\_ALGORITHM\_OBJ) NULL\_PTR for decrypting algorithms that do not need random numbers. The surrender context for processing and canceling during lengthy operations is *surrenderContext*; if its value is (A\_SURRENDER\_CTX \*) NULL\_PTR, Crypto-C does not use it. B\_DecryptUpdate may be called zero or more times to supply the data by parts. See B\_DecryptInit.

### Return value

---

Value	Description
0	Operation was successful.
non-zero	see Appendix A, "Crypto-C Error Types"

---

---

## B\_DestroyAlgorithmObject

```
void B_DestroyAlgorithmObject (  
    B_ALGORITHM_OBJ *algorithmObject           /* pointer to algorithm object */  
);
```

### Description

*B\_DestroyAlgorithmObject* destroys *algorithmObject*, zeroizing any sensitive information, freeing the memory the algorithm object occupied, and setting *algorithmObject* to (B\_ALGORITHM\_OBJ)NULL\_PTR. If *algorithmObject* is already (B\_ALGORITHM\_OBJ)NULL\_PTR or is not a valid algorithm object, no action is taken. See *B\_CreateAlgorithmObject*.

After this routine is called, all the pointers to information blocks returned by calls to *B\_GetAlgorithmInfo* will no longer be valid, since the memory associated with those blocks will have been zeroed and freed.

### Return value

There is no return value.

## B\_DestroyKeyObject

```
void B_DestroyKeyObject (  
    B_KEY_OBJ *keyObject                                     /* pointer to key object */  
);
```

### Description

*B\_DestroyKeyObject* destroys *keyObject*, zeroizing any sensitive information, freeing the memory the key object occupied, and setting *keyObject* to (B\_KEY\_OBJ)NULL\_PTR. If *keyObject* is already (B\_KEY\_OBJ)NULL\_PTR or is not a valid key object, no action is taken. See *B\_CreateKeyObject*.

After this routine is called, all the pointers to information blocks returned by calls to *B\_GetKeyInfo* will no longer be valid, since the memory associated with those blocks will have been zeroed and freed.

### Return value

There is no return value.

## B\_DigestFinal

```

int B_DigestFinal (
    B_ALGORITHM_OBJ algorithmObject,           /* algorithm object */
    unsigned char digest,                      /* message digest output buffer */
    unsigned int digestLen,                    /* length of message digest output */
    unsigned int maxDigestLen,                /* size of output buffer */
    A_SURRENDER_CTX surrenderContext         /* surrender context */
);

```

### Description

`B_DigestFinal` finalizes the digesting process for *algorithmObject* and writes the message digest to *digest*, which is a buffer supplied by the caller of at least *maxDigestLen* bytes, and sets *digestLen* to the length of the digest. The surrender context for processing and canceling during lengthy operations is *surrenderContext*; if its value is `(A_SURRENDER_CTX *)NULL_PTR`, Crypto-C does not use it. *algorithmObject* is reset to the state it was in after the call to `B_DigestInit`, so that another message digesting process may be performed.

### Return value

Value	Description
0	Operation was successful.
non-zero	see Appendix A, "Crypto-C Error Types"

## B\_DigestInit

```
int B_DigestInit (
    B_ALGORITHM_OBJ      algorithmObject,          /* algorithm object */
    B_KEY_OBJ            keyObject,                /* key object */
    B_ALGORITHM_CHOOSER algorithmChooser,         /* algorithm chooser */
    A_SURRENDER_CTX     surrenderContext          /* surrender context */
);
```

### Description

`B_DigestInit` initializes *algorithmObject* for computing a message digest using the algorithm specified by a previous call to `B_SetAlgorithmInfo`. The chooser for selecting the algorithm method is *algorithmChooser*. The key object for supplying the key information is *keyObject*; it should be `(B_KEY_OBJ)NULL_PTR` for keyless digesting algorithms. The surrender context for processing and canceling during lengthy operations is *surrenderContext*; if its value is `(A_SURRENDER_CTX *)NULL_PTR`, Crypto-C does not use it.

`B_DigestInit` only needs to be called once to set up a digest algorithm. The `B_DigestUpdate` routine can be called multiple times to process blocks of data, and `B_DigestFinal` is called once to process the last block which includes producing the result. After `B_DigestFinal` is called, `B_DigestUpdate` can be called to start digesting another sequence of blocks. There is no need to call `B_DigestInit` again.

### Return value

---

Value	Description
0	Operation was successful.
non-zero	see Appendix A, "Crypto-C Error Types"

---

## B\_DigestUpdate

```
int B_DigestUpdate (
    B_ALGORITHM_OBJ algorithmObject,          /* algorithm object */
    unsigned char *partIn,                    /* input data */
    unsigned int partInLen,                  /* length of input data */
    A_SURRENDER_CTX *surrenderContext        /* surrender context */
);
```

### Description

*B\_DigestUpdate* updates *algorithmObject* with *partInLen* bytes from *partIn*. The surrender context for processing and canceling during lengthy operations is *surrenderContext*; if its value is (A\_SURRENDER\_CTX \*)NULL\_PTR, Crypto-C does not use it. *B\_DigestUpdate* may be called zero or more times to supply the data by parts. See *B\_DigestInit*.

### Return value

Value	Description
0	Operation was successful.
non-zero	see Appendix A, "Crypto-C Error Types"

## B\_EncodeDigestInfo

```
int B_EncodeDigestInfo (
    unsigned char *digestInfo,           /* encoded output buffer */
    unsigned int *digestInfoLen,        /* length of encoded output */
    unsigned int maxDigestInfoLen,     /* size of digestInfo buffer */
    ITEM *algorithmID,                  /* message digest algorithm identifier */
    unsigned char *digest,              /* message digest value */
    unsigned int digestLen              /* length of digest */
);
```

### Description

B\_EncodeDigestInfo encodes the DER encoding of a PKCS #1 DigestInfo type, writing the encoding to *digestInfo*, which is a buffer supplied by the caller of at least *maxDigestInfoLen* bytes, and sets *digestInfoLen* to the length of the encoding. *algorithmID* points to an ITEM that gives the DER encoding of the message digest algorithm. The ITEM type is defined by the KI\_ITEM key info type in Chapter 3. Typically, *algorithmID* is the value of *info* returned by calling B\_GetAlgorithmInfo. *digest* points to the message digest value of length *digestLen*. Typically, *digest* is returned by B\_DigestFinal.

### Return value

---

Value	Description
0	Operation was successful.
non-zero	see Appendix A, "Crypto-C Error Types"

---

## B\_EncodeFinal

```
int B_EncodeFinal (
    B_ALGORITHM_OBJ algorithmObject,           /* algorithm object */
    unsigned char *partOut,                    /* output data buffer */
    unsigned int *partOutLen,                 /* length of output data */
    unsigned int maxPartOutLen                /* size of output data buffer */
);
```

### Description

B\_EncodeFinal finalizes the encoding process specified by *algorithmObject*, writing any remaining encoded output to *partOut*, which is a buffer supplied by the caller of at least *maxPartOutLen* bytes, and setting *partOutLen* to the number of bytes written to *partOut*. *algorithmObject* is reset to the state it was in after the call to B\_EncodeInit, so that another encoding process may be performed. See B\_EncodeInit.

### Return value

Value	Description
0	Operation was successful.
non-zero	see Appendix A, "Crypto-C Error Types"

## B\_EncodeInit

```
int B_EncodeInit (  
    B_ALGORITHM_OBJ algorithmObject /* algorithm object */  
);
```

### Description

`B_EncodeInit` initializes *algorithmObject* for encoding data using the algorithm specified by a previous call to `B_SetAlgorithmInfo`. For example, the `AI_RFC1113Recode` algorithm provides Base64 encoding and decoding to convert binary data to and from a printable form suitable for most email systems. Notice that there are no cryptographic keys for encoding or decoding.

`B_EncodeInit` only needs to be called once to set up a Encode algorithm. The `B_EncodeUpdate` routine can be called multiple times to process blocks of data, and `B_EncodeFinal` is called once to process the last block which includes adding any trailing pad bytes. After `B_EncodeFinal` is called, `B_EncodeUpdate` can be called to start decoding another sequence of blocks. There is no need to call `B_EncodeInit` again.

### Return value

---

Value	Description
0	Operation was successful.
non-zero	see Appendix A, "Crypto-C Error Types"

---

## B\_EncodeUpdate

```

int B_EncodeUpdate (
    B_ALGORITHM_OBJ algorithmObject,          /* algorithm object */
    unsigned char *partOut,                    /* output data buffer */
    unsigned int *partOutLen,                 /* length of output data */
    unsigned int maxPartOutLen,              /* size of output data buffer */
    unsigned char *partIn,                    /* input data */
    unsigned int partInLen,                  /* length of input data */
);

```

### Description

B\_EncodeUpdate updates the encoding process specified by *algorithmObject* with *partInLen* bytes from *partIn*, writing the encoded output to *partOut*, which is a buffer supplied by the caller of at least *maxPartOutLen* bytes, and setting *partOutLen* to the number of bytes written to *partOut*. B\_EncodeUpdate may be called zero or more times to supply the data by parts. See B\_EncodeInit.

### Return value

Value	Description
0	Operation was successful.
non-zero	see Appendix A, "Crypto-C Error Types"

## B\_EncryptFinal

```
int B_EncryptFinal (
    B_ALGORITHM_OBJ algorithmObject,           /* algorithm object */
    unsigned char *partOut,                   /* output data buffer */
    unsigned int *partOutLen,                 /* length of output data */
    unsigned int maxPartOutLen,              /* size of output data buffer */
    B_ALGORITHM_OBJ randomAlgorithm,         /* random byte source */
    A_SURRENDER_CTX *surrenderContext        /* surrender context */
);
```

### Description

`B_EncryptFinal` finalizes the encrypting process specified by `algorithmObject`, writing any remaining encrypted output to `partOut`, which is a buffer supplied by the caller of at least `maxPartOutLen` bytes, and setting `partOutLen` to the number of bytes written to `partOut`. The algorithm object for supplying random numbers is `randomAlgorithm`, it may be `(B_ALGORITHM_OBJ) NULL_PTR` for encrypting algorithms that do not need random numbers. The surrender context for processing and canceling during lengthy operations is `surrenderContext`; if its value is `(A_SURRENDER_CTX *) NULL_PTR`, Crypto-C does not use it. `algorithmObject` is reset to the state it was in after the call to `B_EncryptInit`, so that another encrypting process may be performed. See `B_EncryptInit`.

### Return value

---

Value	Description
0	Operation was successful.
non-zero	see Appendix A, "Crypto-C Error Types"

---

## B\_EncryptInit

```
int B_EncryptInit (
    B_ALGORITHM_OBJ      algorithmObject,          /* algorithm object */
    B_KEY_OBJ            keyObject,                /* key object */
    B_ALGORITHM_CHOOSER algorithmChooser,         /* algorithm chooser */
    A_SURRENDER_CTX     *surrenderContext          /* surrender context */
);
```

### Description

B\_EncryptInit initializes *algorithmObject* for encrypting data using the algorithm specified by a previous call to B\_SetAlgorithmInfo. The key object for supplying the key information is *keyObject*. The chooser for selecting the algorithm method is *algorithmChooser*. The surrender context for processing and canceling during lengthy operations is *surrenderContext*; if its value is (A\_SURRENDER\_CTX \*)NULL\_PTR, Crypto-C does not use it.

B\_EncryptInit only needs to be called once to set up a key. The B\_EncryptUpdate routine can be called multiple times to process blocks of data, and B\_EncryptFinal is called once to process the last block, which includes adding the trailing pad bytes. After B\_EncryptFinal is called, B\_EncryptUpdate can be called to start processing another sequence of blocks. If a different CBC Initialization Vector (IVs) is used with each sequence of blocks, B\_SetAlgorithmInfo can be called with AI\_CBC\_IV8 to set the new IV before calling B\_EncryptUpdate. There is no need to call B\_EncryptInit again with the same key.

### Return value

Value	Description
0	Operation was successful.
non-zero	see Appendix A, "Crypto-C Error Types"

## B\_EncryptUpdate

```

int B_EncryptUpdate (
    B_ALGORITHM_OBJ algorithmObject,           /* algorithm object */
    unsigned char *partOut,                    /* output data buffer */
    unsigned int *partOutLen,                  /* length of output data */
    unsigned int maxPartOutLen,               /* size of output data buffer */
    unsigned char *partIn,                     /* input data */
    unsigned int partInLen,                   /* length of input data */
    B_ALGORITHM_OBJ randomAlgorithm,         /* random byte source */
    A_SURRENDER_CTX *surrenderContext        /* surrender context */
);

```

### Description

B\_EncryptUpdate updates the encrypting process specified by *algorithmObject* with *partInLen* bytes from *partIn*, writing the encrypted output to *partOut*, which is a buffer supplied by the caller of at least *maxPartOutLen* bytes, and setting *partOutLen* to the number of bytes written to *partOut*. The algorithm object for supplying random numbers is *randomAlgorithm*; it may be (B\_ALGORITHM\_OBJ) NULL\_PTR for encrypting algorithms that do not need random numbers. The surrender context for processing and canceling during lengthy operations is *surrenderContext*; if its value is (A\_SURRENDER\_CTX \*) NULL\_PTR, Crypto-C does not use it. B\_EncryptUpdate may be called zero or more times to supply the data by parts.

### Return value

Value	Description
0	Operation was successful.
non-zero	see Appendix A, "Crypto-C Error Types"

## B\_FreeSessionChooser



```
int B_FreeSessionChooser (
    B_ALGORITHM_CHOOSER *sessionChooser,          /* Address of runtime chooser */
                                                    /* dynamically bound to available */
                                                    /* hardware-based methods */
    unsigned char    ***oemTagList,              /* Address of list of OEM */
                                                    /* hardware method tags */
);
```

### Description

*B\_FreeSessionChooser* frees the memory allocated in the process of creating *sessionChooser* and *oemTagList*. Whenever a non-null information pointer from the extended AM is encountered, its corresponding Final function is called to destroy it.

### Return value

Value	Description
0	Operation was successful.
nonzero	unsuccessful, allocation error

## B\_GenerateInit

```
int B_GenerateInit (  
    B_ALGORITHM_OBJ algorithmObject,           /* algorithm object */  
    B_ALGORITHM_CHOOSER algorithmChooser,      /* algorithm chooser */  
    A_SURRENDER_CTX surrenderContext          /* surrender context */  
);
```

### Description

`B_GenerateInit` initializes *algorithmObject* using the algorithm specified by a previous call to `B_SetAlgorithmInfo`. The chooser for selecting the algorithm method is *algorithmChooser*. The surrender context for processing and canceling during lengthy operations is *surrenderContext*; if its value is `(A_SURRENDER_CTX *)NULL_PTR`, Crypto-C does not use it.

This routine is used to initialize several of the toolkit's parameter generation algorithms like `B_GenerateKeyPair` or `B_GenerateParameters`. However, `B_RandomInit` is used to initialize the generator for `B_GenerateRandomBytes`.

### Return value

---

Value	Description
0	Operation was successful.
non-zero	see Appendix A, "Crypto-C Error Types"

---

## B\_GenerateKeypair

```
int B_GenerateKeypair (
    B_ALGORITHM_OBJ algorithmObject,          /* algorithm object */
    B_KEY_OBJ publicKey,                      /* new public key */
    B_KEY_OBJ privateKey,                    /* new private key */
    B_ALGORITHM_OBJ randomAlgorithm,        /* random algorithm */
    A_SURRENDER_CTX surrenderContext        /* surrender context */
);
```

### Description

B\_GenerateKeypair uses *algorithmObject* to generate a keypair, setting *publicKey* and *privateKey* to the result. The algorithm object for supplying random numbers is *randomAlgorithm*. The surrender context for processing and canceling during lengthy operations is *surrenderContext*; if its value is (A\_SURRENDER\_CTX \*)NULL\_PTR, Crypto-C does not use it. *algorithmObject* is reset to the state it was in after the call to B\_GenerateInt, so that another keypair generation may be performed. See B\_GenerateInt.

### Return value

Value	Description
0	Operation was successful.
non-zero	see Appendix A, "Crypto-C Error Types"

## B\_GenerateParameters

```
int B_GenerateParameters (
    B_ALGORITHM_OBJ algorithmObject,           /* algorithm object */
    B_ALGORITHM_OBJ resultAlgorithmObject,     /* result algorithm object */
    B_ALGORITHM_OBJ randomAlgorithmObject,    /* random algorithm */
    A_SURRENDER_CTX surrenderContext         /* surrender context */
);
```

### Description

B\_GenerateParameters uses *algorithmObject* to generate algorithm parameters, setting *resultAlgorithmObject* to the result. The application may then use B\_GetAlgorithmInfo to get the new parameters from *resultAlgorithmObject*. The algorithm object for supplying random numbers is *randomAlgorithmObject*. The surrender context for processing and canceling during lengthy operations is *surrenderContext*; if its value is (A\_SURRENDER\_CTX \*)NULL\_PTR, Crypto-C does not use it. *algorithmObject* is reset to the state it was in after the call to B\_GenerateInit, so that another parameter generation may be performed. See B\_GenerateInit.

### Return value

---

Value	Description
0	Operation was successful.
non-zero	see Appendix A, "Crypto-C Error Types"

---

## B\_GenerateRandomBytes

```

int B_GenerateRandomBytes (
    B_ALGORITHM_OBJ randomAlgorithm,           /* random algorithm */
    unsigned char *output,                     /* buffer for output bytes */
    unsigned int outputLen,                   /* number of bytes to output */
    A_SURRENDER_CTX *surrenderContext        /* surrender context */
);

```

### Description

`B_GenerateRandomBytes` generates *outputLen* pseudo-random bytes from *randomAlgorithm*, storing the result in *output*. The *randomAlgorithm* must have been seeded. The surrender context for processing and canceling during lengthy operations is *surrenderContext*; if its value is `(A_SURRENDER_CTX *)NULL_PTR`, Crypto-C does not use it. See `B_RandomInt`.

### Return value

Value	Description
0	Operation was successful.
non-zero	see Appendix A, "Crypto-C Error Types"

## B\_GetAlgorithmInfo

```
int B_GetAlgorithmInfo (
    POINTER *info, /* algorithm information */
    B_ALGORITHM_OBJ algorithmObject, /* algorithm object */
    B_INFO_TYPE infoType /* type of algorithm information */
);
```

### Description

B\_GetAlgorithmInfo gets the information held by *algorithmObject* in the format specified by *infoType*, storing the result in *info*. The value of *infoType* is one of the algorithm info types with an AI\_ prefix listed in Chapter 2. The format of the information returned by B\_GetAlgorithmInfo is the same as the format supplied to B\_SetAlgorithmInfo.

This routine can be used to convert between external representations of information. For example, an algorithm can be set up to perform encryption using AI\_MD2WithDES\_CBCPad, and later the BER representation of that algorithm can be computed by calling B\_GetAlgorithmInfo with AI\_MD2WithDES\_CBCPadBER. These external representations of algorithm identifiers are used in RSA Data Security, Inc.'s PKCS standards and other industry cryptographic standards.

### Return value

---

Value	Description
0	Operation was successful.
non-zero	see Appendix A, "Crypto-C Error Types"

---

## B\_GetExtendedErrorInfo



```

void B_GetExtendedErrorInfo (
    B_ALGORITHM_OBJ algorithmObj,           /* algorithm object */
    ITEM             *errorDataItem,       /* returns pointer to error data */
                                                    /* and length of data */
    POINTER         *AM                    /* Set to point at method table */
);

```

### Description

B\_GetExtendedErrorInfo sets *errorDataItem->data* to point at the error data, and *errorDataItem->len* to the length in bytes of the error data. *AM* is set to the address of the algorithm method that originated the error if any.

### Notes:

A NULL extended error is indicated by a length of zero. The error data may in reality be a data structure that includes pointers to allocated memory. These allocations are cleaned up using an error destruction routine assigned during the creation of the extended error data.

### Return value

There is no return value.

## B\_GetKeyExtendedErrorInfo



```
void B_GetKeyExtendedErrorInfo (  
    B_KEY_OBJ keyObject,                               /* key object */  
    ITEM      *errorDataItem,                          /* returns pointer to */  
                                                       /* error data and length of data */  
    POINTER   *AM,                                       /* Set to point at method table */  
);
```

### Description

*B\_GetKeyExtendedErrorInfo* sets *errorDataItem->data* to point at the error data, and *errorDataItem->len* to the length in bytes of the error data. *AM* is optionally set by the hardware manufacturer; consult the documentation supplied by your hardware vendor for more information.

### Notes:

A null extended error is indicated by a length of zero. The error data may in reality be a data structure that includes pointers to allocated memory. These allocations are cleaned up using an error destruction routine assigned during the creation of the extended error data.

### Return value

There is no return value.

## B\_GetKeyInfo

```
int B_GetKeyInfo (
    POINTER *info,                /* key information */
    B_KEY_OBJ keyObject,         /* key object */
    B_INFO_TYPE infoType        /* type of key information */
);
```

### Description

B\_GetKeyInfo gets the information held by *keyObject* in the format specified by *infoType*, storing the result in *info*. The value of *infoType* is one of the key info types with a KI\_ prefix listed in Chapter 3. The format of the information returned by B\_GetKeyInfo is not always identical to the format supplied to B\_SetKeyInfo because B\_SetKeyInfo may canonicalize the information before it stores it in the key object. For example, KI\_DES8 sets the DES parity before storing, KI\_RSAPublicBER converts a BER encoding to DER, and KI\_RSAPublic strips off leading zeros from the modulus and exponent integers.

### Return value

Value	Description
0	Operation was successful.
non-zero	see Appendix A, "Crypto-C Error Types"

## B\_IntegerBits

```
unsigned int B_IntegerBits (  
    unsigned char *integer,                /* canonical integer */  
    unsigned int  integerLen              /* length in bytes */  
);
```

### Description

*B\_IntegerBits* returns the number of significant bits in an arbitrary-length integer, where *integer* points to an unsigned byte array, most significant byte first and *integerLen* gives its length. Leading zeroes are ignored. The integer is considered unsigned; that is, the most-significant bit is counted and is not considered a sign bit. If *integerLen* is zero, *integer* is ignored and *B\_IntegerBits* returns zero. A typical application uses *B\_IntegerBits* to determine the key size in bits of an RSA key by passing in the modulus.

This routine can be used to examine the value of a large integer such as the ones returned by *B\_GetKeyInfo* for KI's like *KI\_RSAPublic*.

### Return value

*B\_IntegerBits* returns the number of significant bits in *integer*.

## B\_KeyAgreeInit

```

int B_KeyAgreeInit (
    B_ALGORITHM_OBJ algorithmObject, /* algorithm object */
    B_KEY_OBJ keyObject, /* key object */
    B_ALGORITHM_CHOOSER algorithmChooser, /* algorithm chooser */
    A_SURRENDER_CTX surrenderContext /* surrender context */
);

```

### Description

`B_KeyAgreeInit` initializes *algorithmObject* for performing key agreement using the algorithm specified by a previous call to `B_SetAlgorithmInfo`. The chooser for selecting the algorithm method is *algorithmChooser*. The key object for supplying the key information is *keyObject*; it should be `(B_KEY_OBJ) NULL_PTR` for key agreement algorithms that do not need an input key. The surrender context for processing and canceling during lengthy operations is *surrenderContext*; if its value is `(A_SURRENDER_CTX *) NULL_PTR`, Crypto-C does not use it.

This routine can be used for Diffie-Hellman key agreement. First `B_KeyAgreeInit` is called to setup the algorithm, then each party calls `B_KeyAgreePhase1` to generate the value that is then sent to the other party. Each party then passes the received value to `B_KeyAgreePhase2`, which computes the agreed upon key. If several key agreements are done using the same algorithm, there is no need to call `B_KeyAgreeInit` again.

### Return value

Value	Description
0	Operation was successful.
non-zero	see Appendix A, "Crypto-C Error Types"

## B\_KeyAgreePhase1

```
int B_KeyAgreePhase1 (
    B_ALGORITHM_OBJ algorithmObject,           /* algorithm object */
    unsigned char   *output,                   /* output data buffer */
    unsigned int    *outputLen,               /* length of output data */
    unsigned int    maxOutputLen,            /* size of output data buffer */
    B_ALGORITHM_OBJ randomAlgorithm,         /* random byte source */
    A_SURRENDER_CTX *surrenderContext        /* surrender context */
);
```

### Description

B\_KeyAgreePhase1 uses *algorithmObject* to generate the initial value for the other party, writing it to *output*, which is a buffer supplied by the caller of at least *maxOutputLen* bytes, and setting *outputLen* to the number of bytes written to *output*. The algorithm object for supplying random numbers is *randomAlgorithm*. The surrender context for processing and canceling during lengthy operations is *surrenderContext*; if its value is (A\_SURRENDER\_CTX \*)NULL\_PTR, Crypto-C does not use it. See B\_KeyAgreeInit.

### Return value

---

Value	Description
0	Operation was successful.
non-zero	see Appendix A, "Crypto-C Error Types"

---

## B\_KeyAgreePhase2

```

int B_KeyAgreePhase2 (
    B_ALGORITHM_OBJ algorithmObject,           /* algorithm object */
    unsigned char *output,                       /* output data buffer */
    unsigned int *outputLen,                     /* length of output data */
    unsigned int maxOutputLen,                   /* size of output data buffer */
    unsigned char *input,                         /* input data */
    unsigned int inputLen,                       /* length of input data */
    A_SURRENDER_CTX *surrenderContext           /* surrender context */
);

```

### Description

B\_KeyAgreePhase2 performs a round of key agreement as specified by *algorithmObject*, receiving *inputLen* bytes from *input*, which is the other party's intermediate value. B\_KeyAgreePhase2 writes the output to *output*, which is a buffer supplied by the caller of at least *maxOutputLen* bytes, and sets *outputLen* to the number of bytes written to *output*. If *input* is the other party's final intermediate value, *output* is the agreed-upon key; otherwise, *output* is a new intermediate value to send to the other party. The surrender context for processing and canceling during lengthy operations is *surrenderContext*; if its value is (A\_SURRENDER\_CTX \*)NULL\_PTR, Crypto-C does not use it.

B\_KeyAgreePhase2 may be called one or more times to process intermediate values, depending on how many other parties are involved in the key agreement. For an algorithm like Diffie-Hellman, B\_KeyAgreePhase2 is called once.

### Return value

Value	Description
0	Operation was successful.
non-zero	see Appendix A, "Crypto-C Error Types"

## B\_RandomInit

```
int B_RandomInit (
    B_ALGORITHM_OBJ      randomAlgorithm,          /* random algorithm object */
    B_ALGORITHM_CHOOSER algorithmChooser,         /* algorithm chooser */
    A_SURRENDER_CTX     surrenderContext         /* surrender context */
);
```

### Description

B\_RandomInit initializes *randomAlgorithm* for generating random bytes using the algorithm specified by a previous call to B\_SetAlgorithmInfo. *randomAlgorithm* is ready to generate bytes after the call to B\_RandomInit. However, it is necessary to mix in random seed values with B\_RandomUpdate. Otherwise, without seed values, the bytes generated by the algorithm follow a default unseeded byte sequence. The chooser for selecting the algorithm method is *algorithmChooser*. The surrender context for processing and canceling during lengthy operations is *surrenderContext*; if its value is (A\_SURRENDER\_CTX \*)NULL\_PTR, Crypto-C does not use it.

B\_RandomInit is called once to create the generator, then B\_RandomUpdate is called one or more times to add "seed" bytes (values that are hard for an attacker to predict) to the generator. After enough seed is added, say at least 128 bytes, then B\_GenerateRandomBytes can be called one or more times to generate blocks of pseudo-random data. If B\_RandomUpdate is only called once before B\_GenerateRandomBytes, then the BSAFE 2 algorithms will be used. Two or more calls to B\_RandomUpdate will cause the improved BSAFE 3 algorithms to be used. It is also OK to call B\_RandomUpdate after calling B\_GenerateRandomBytes in order to add more hard to predict values to the generator. There is no need to call B\_RandomInit again.

### Return value

---

Value	Description
0	Operation was successful.
non-zero	see Appendix A, "Crypto-C Error Types"

---

## B\_RandomUpdate

```
int B_RandomUpdate (
    B_ALGORITHM_OBJ randomAlgorithm,          /* random algorithm */
    unsigned char *input,                    /* block values to mix in */
    unsigned int inputLen,                  /* length of input block */
    A_SURRENDER_CTX *surrenderContext      /* surrender context */
);
```

### Description

`B_RandomUpdate` mixes *inputLen* bytes from *input* into *randomAlgorithm*. The surrender context for processing and canceling during lengthy operations is *surrenderContext*; if its value is `(A_SURRENDER_CTX *)NULL_PTR`, Crypto-C does not use it. See `B_RandomInit`.

### Return value

Value	Description
0	Operation was successful.
non-zero	see Appendix A, "Crypto-C Error Types"

## B\_SetAlgorithmInfo

```
int B_SetAlgorithmInfo (
    B_ALGORITHM_OBJ algorithmObject,          /* algorithm object */
    B_INFO_TYPE     infoType,                /* type of algorithm information */
    POINTER         info                    /* algorithm information */
);
```

### Description

B\_SetAlgorithmInfo sets the parameters of *algorithmObject* to the information pointed to by *info*. The type of algorithm and the format of the parameters is specified by *infoType*, which is one of the algorithm info types with an AI\_ prefix listed in Chapter 2. A separate copy of the information supplied by *info* is allocated inside the algorithm object so that *info* may be changed after the call to B\_SetAlgorithmInfo. B\_SetAlgorithmInfo returns BE\_WRONG\_ALGORITHM\_INFO if the algorithm type encoded in *info* is not the type expected by *infoType*.

Once an algorithm object has been set, it should not be reset, that is, do not call B\_SetAlgorithmInfo twice on a single created algorithm object. Either create a new algorithm object or destroy an existing one and create it again.

### Return value

---

Value	Description
0	Operation was successful.
non-zero	see Appendix A, "Crypto-C Error Types"

---

## B\_SetKeyInfo

```
int B_SetKeyInfo (
    B_KEY_OBJ keyObject, /* key object */
    B_INFO_TYPE infoType, /* type of key information */
    POINTER info /* key information */
);
```

### Description

B\_SetKeyInfo sets the value of *keyObject* to the information pointed to by *info*. The format of the information is specified by *infoType*, which is one of the key info types with a KI\_ prefix listed in Chapter 3. Also, some of the AI algorithm info types listed in Chapter 2 specify the key info type that should be used to set the key object needed by the algorithm. A separate copy of the information supplied by *info* is allocated inside the key object so that *info* may be changed after the call to B\_SetKeyInfo. B\_SetKeyInfo returns BE\_WRONG\_KEY\_INFO if the key type encoded in *info* is not the type expected by *infoType*.

Once a key object has been set, it should not be reset, that is, do not call B\_SetKeyInfo twice on a single created key object. Either create a new key object or destroy an existing one and create it again.

### Return value

Value	Description
0	Operation was successful.
non-zero	see Appendix A, "Crypto-C Error Types"

## B\_SignFinal

```
int B_SignFinal (  
    B_ALGORITHM_OBJ algorithmObject,           /* algorithm object */  
    unsigned char signature,                 /* signature output buffer */  
    unsigned int signatureLen,               /* length of signature output */  
    unsigned int maxSignatureLen,           /* size of output buffer */  
    B_ALGORITHM_OBJ randomAlgorithm,        /* random byte source */  
    A_SURRENDER_CTX surrenderContext        /* surrender context */  
);
```

### Description

`B_SignFinal` finalizes the digesting process for *algorithmObject* and computes the digital signature, writing the signature to *signature*, which is a buffer supplied by the caller of at least *maxSignatureLen* bytes, and sets *signatureLen* to the length of the signature. The algorithm object for supplying random numbers is *randomAlgorithm*, it may be (B\_ALGORITHM\_OBJ) NULL\_PTR for signature algorithms that do not need random numbers. The surrender context for processing and canceling during lengthy operations is *surrenderContext*; if its value is (A\_SURRENDER\_CTX \*) NULL\_PTR, Crypto-C does not use it. *algorithmObject* is reset to the state it was in after the call to `B_SignInit`, so that another signing process may be performed.

### Return value

---

Value	Description
0	Operation was successful.
non-zero	see Appendix A, "Crypto-C Error Types"

---

## B\_SignInit

```
int B_SignInit (
    B_ALGORITHM_OBJ      algorithmObject,      /* algorithm object */
    B_KEY_OBJ            keyObject,           /* key object */
    B_ALGORITHM_CHOOSER algorithmChooser,     /* algorithm chooser */
    A_SURRENDER_CTX     *surrenderContext     /* surrender context */
);
```

### Description

`B_SignInit` initializes *algorithmObject* for computing a digital signature using the algorithm specified by a previous call to `B_SetAlgorithmInfo`. The chooser for selecting the algorithm method is *algorithmChooser*. The key object for supplying the key information is *keyObject*, which is typically a private key. The surrender context for processing and canceling during lengthy operations is *surrenderContext*; if its value is `(A_SURRENDER_CTX *)NULL_PTR`, Crypto-C does not use it.

`B_SignInit` only needs to be called once to set up a signature algorithm. The `B_SignUpdate` routine can be called multiple times to process blocks of data, and `B_SignFinal` is called once to process the last block which includes producing the result. After `B_SignFinal` is called, `B_SignUpdate` can be called to start signing another sequence of blocks. There is no need to call `B_SignInit` again.

### Return value

Value	Description
0	Operation was successful.
non-zero	see Appendix A, "Crypto-C Error Types"

## B\_SignUpdate

```
int B_SignUpdate (  
    B_ALGORITHM_OBJ algorithmObject,           /* algorithm object */  
    unsigned char *partIn,                     /* input data */  
    unsigned int partInLen,                   /* length of input data */  
    A_SURRENDER_CTX *surrenderContext        /* surrender context */  
);
```

### Description

*B\_SignUpdate* updates the digesting process for *algorithmObject* with *partInLen* bytes from *partIn*. The surrender context for processing and canceling during lengthy operations is *surrenderContext*; if its value is (A\_SURRENDER\_CTX \*)NULL\_PTR, Crypto-C does not use it. *B\_SignUpdate* may be called zero or more times to supply the data by parts. See *B\_SignInit*.

### Return value

---

Value	Description
0	Operation was successful.
non-zero	Error. See Appendix A, "Crypto-C Error Types."

---

## B\_SymmetricKeyGenerate



```
int B_SymmetricKeyGenerate (
    B_ALGORITHM_OBJ algorithmObject,
    B_KEY_OBJ symmetricKey,
    B_ALGORITHM_OBJ randomObject,
    A_SURRENDER_CTX *surrenderContext;
);
```

### Description

Creates a symmetric key in accordance with data specified during the B\_SetAlgorithmInfo step. If hardware is present, the key information is stored in a KI\_TOKEN\_INFO structure. If no hardware is present, the key information is stored in KI\_EXTENDED\_TOKEN\_INFO format, which extends the KI-Token base type.

### Return value

Value	Description
0	Operation was successful.
nonzero	Error. See Appendix A, "Crypto-C Error Types."

## B\_SymmetricKeyGenerateInit

```
int B_SymmetricKeyGenerateInit (  
    B_ALGORITHM_OBJ algorithmObject,  
    B_ALGORITHM_CHOOSER algorithmChooser,  
    A_SURRENDER_CTX *surrenderContext  
);
```

### Description

Initializes key generation object.

### Return value

---

Value	Description
0	Operation was successful.
nonzero	error

---

## B\_VerifyFinal

```

int B_VerifyFinal (
    B_ALGORITHM_OBJ algorithmObject,           /* algorithm object */
    unsigned char *signature,                 /* signature to verify */
    unsigned int signatureLen,               /* length of signature */
    B_ALGORITHM_OBJ randomAlgorithm,        /* random byte source */
    A_SURRENDER_CTX *surrenderContext       /* surrender context */
);

```

### Description

B\_VerifyFinal finalizes the digesting process for *algorithmObject* and verifies the digital signature supplied by *signature* of *signatureLen* bytes. The algorithm object for supplying random numbers is *randomAlgorithm*, it may be (B\_ALGORITHM\_OBJ) NULL\_PTR for signature algorithms that do not need random numbers. The surrender context for processing and canceling during lengthy operations is *surrenderContext*, if its value is (A\_SURRENDER\_CTX \*) NULL\_PTR, Crypto-C does not use it. *algorithmObject* is reset to the state it was in after the call to B\_VerifyFinal, so that another verifying process may be performed. See B\_VerifyFinal.

### Return value

Value	Description
0	Operation was successful.
non-zero	see Appendix A, "Crypto-C Error Types"

## B\_VerifyInit

```
int B_VerifyInit (
    B_ALGORITHM_OBJ      algorithmObject,          /* algorithm object */
    B_KEY_OBJ            keyObject,                /* key object */
    B_ALGORITHM_CHOOSER algorithmChooser,         /* algorithm chooser */
    A_SURRENDER_CTX     surrenderContext          /* surrender context */
);
```

### Description

`B_VerifyInit` initializes *algorithmObject* for verifying a digital signature using the algorithm specified by a previous call to `B_SetAlgorithmInfo`. The chooser for selecting the algorithm method is *algorithmChooser*. The key object for supplying the key information is *keyObject*, which is typically a public key. The surrender context for processing and canceling during lengthy operations is *surrenderContext*; if its value is `(A_SURRENDER_CTX *)NULL_PTR`, Crypto-C does not use it.

`B_VerifyInit` only needs to be called once to set up a verification algorithm. The `B_VerifyUpdate` routine can be called multiple times to process blocks of data, and `B_VerifyFinal` is called once to process the last block which includes checking the computed signature against the expected signature that is passed to `B_VerifyFinal`. After `B_VerifyFinal` is called, `B_VerifyUpdate` can be called to start verifying another sequence of blocks. There is no need to call `B_VerifyInit` again.

### Return value

---

Value	Description
0	Operation was successful.
non-zero	see Appendix A, "Crypto-C Error Types"

---

## B\_VerifyUpdate

```
int B_VerifyUpdate (
    B_ALGORITHM_OBJ algorithmObject,           /* algorithm object */
    unsigned char *partIn,                      /* input data */
    unsigned int partInLen,                    /* length of input data */
    A_SURRENDER_CTX *surrenderContext         /* surrender context */
);
```

### Description

B\_VerifyUpdate updates the digesting process for *algorithmObject* with *partInLen* bytes from *partIn*. The surrender context for processing and canceling during lengthy operations is *surrenderContext*; if its value is (A\_SURRENDER\_CTX \*)NULL\_PTR, Crypto-C does not use it. B\_VerifyUpdate may be called zero or more times to supply the data by parts. See B\_VerifyInit.

### Return value

Value	Description
0	Operation was successful.
non-zero	see Appendix A, "Crypto-C Error Types"

## T\_free

```
void T_free (  
    POINTER block /* block address */  
);
```

### Description

T\_free deallocates *block*. The value of *block* is allocated with T\_malloc or reallocated with T\_realloc, or it is NULL\_PTR. If *block* is NULL\_PTR, T\_free performs no operation.

### Return value

There is no return value.

## T\_malloc

```
POINTER T_malloc (  
    unsigned int len                                /* length of block */  
);
```

### Description

`T_malloc` allocates a memory block of at least *len* bytes. The value of *len* can be zero, in which case `T_malloc` returns a valid non-NULL\_PTR value.

### Return value

---

Value	Description
address of block	Operation was successful.
NULL_PTR	error

---

## T\_memcmp

```
int T_memcmp (
    POINTER firstBlock,          /* first block */
    POINTER secondBlock,       /* second block */
    unsigned int len           /* length of blocks */
);
```

### Description

T\_memcmp compares the first *len* bytes of *firstBlock* and *secondBlock*. The value of *len* can be zero, in which case *firstBlock* and *secondBlock* are undefined and T\_memcmp returns zero. T\_memcmp compares the blocks by scanning the blocks from lowest address to highest until a difference is found. The smaller-valued block is the one with the smaller-valued byte at the point of difference. If no difference is found, then the blocks are equal.

### Return value

---

Value	Description
< 0	<i>firstBlock</i> is smaller.
0	The blocks are equal.
> 0	<i>firstBlock</i> is larger.

---

## T\_memcpy

```
void T_memcpy(  
    POINTER    output,          /* output block */  
    POINTER    input,          /* input block */  
    unsigned int len          /* length of blocks */  
);
```

### Description

T\_memcpy copies the first *len* bytes of *input* to *output*. The value of *len* can be zero, in which case *output* and *input* are undefined. The blocks do not overlap.

### Return value

There is no return value.

## T\_memmove

```
void T_memmove (
    POINTER      output,          /* output block */
    POINTER      input,           /* input block */
    unsigned int len             /* length of blocks */
);
```

### Description

T\_memmove copies the first *len* bytes of *input* to *output*. The blocks can overlap. The value of *len* can be zero, in which case *output* and *input* are undefined.

### Return value

There is no return value.

## T\_memset

```
void T_memset (  
    POINTER output,          /* output block */  
    int value,              /* value */  
    unsigned int len        /* length of block */  
);
```

### Description

*T\_memset* sets the first *len* bytes of *output* to *value*. If the value of *len* is zero, *output* is undefined.

### Return value

There is no return value.

## T\_realloc

```
POINTER T_realloc (
    POINTER      block,                /* block address */
    unsigned int len                   /* new length */
);
```

### Description

`T_realloc` changes the size of *block* to *len*. It allocates a memory block of length *len* bytes, copies as many bytes as possible from the old memory block to the new one, and frees the old block. The address of the new block can be different from the address of the old block. The value of *len* can be zero, in which case `T_realloc` returns a valid non-`NULL_PTR` value. On error, *block* is freed. Note that many implementations of `realloc` do not free the block on error, so `T_realloc` must take care to do this. The value of *block* is allocated with `T_malloc` or reallocated with `T_realloc`, or it is `NULL_PTR`. If *block* is `NULL_PTR`, `T_realloc` performs as `T_malloc`.

### Return value

---

Value	Description
address of new block	Operation was successful.
<code>NULL_PTR</code>	error

---

## T\_strcmp

```
int T_strcmp (  
    const char *string1,           /* first string */  
    const char *string2          /* second string */  
);
```

### Description

T\_strlen compares two strings. The return value indicates the lexicographic relation of *string1* to *string2*.

### Return Value

---

Value	Relationship of <i>string1</i> to <i>string2</i>
< 0	<i>string1</i> is less than <i>string2</i>
0	<i>string1</i> is identical to <i>string2</i>
> 0	<i>string1</i> is greater than <i>string2</i>

---

## T\_strcpy

```
char* T_strcpy (
    char *strDest,                /* destination string */
    char *strSource              /* source string */
);
```

The `T_strcpy` function copies *strSource*, including the terminating NULL character, to the location specified by *strDest*.

### Return Value

The destination string.

## T\_strlen

```
unsigned int T_strlen (  
    char *pStr                                /* null-terminated string */  
);
```

### Description

T\_strlen returns the number of characters in *pStr*, excluding the terminal NULL.

### Return Value

The number of characters in the string.

---

T\_strlen

---

---

## Appendix A

# Crypto-C Error Types

---

This appendix lists the RSA BSAFE Crypto-C (Crypto-C) error types.

Table A-1 **Crypto-C Error Types**

Hex	Decimal	Error Code	Description
0x0200	512	BE_ALGORITHM_ALREADY_SET	the value of the algorithm object has already been set by a call to <code>B_SetAlgorithmInfo</code> or by an algorithm parameter generation
0x0201	513	BE_ALGORITHM_INFO	invalid format for the algorithm information in the algorithm object
0x0202	514	BE_ALGORITHM_NOT_INITIALIZED	algorithm object has not been initialized by a call to the <code>Init</code> procedure
0x0203	515	BE_ALGORITHM_NOT_SET	the algorithm object has not been set by a call to <code>B_SetAlgorithmInfo</code>
0x0204	516	BE_ALGORITHM_OBJ	invalid algorithm object
0x0205	517	BE_ALG_OPERATION_UNKNOWN	unknown operation for an algorithm or algorithm info type
0x0206	518	BE_ALLOC	insufficient memory
0x0207	519	BE_CANCEL	operation was cancelled by the <code>surrender</code> function
0x0208	520	BE_DATA	generic data error

Table A-1 **Crypto-C Error Types**

Hex	Decimal	Error Code	Description
0x0209	521	BE_EXPONENT_EVEN	invalid even value for public exponent in keypair generation
0x020a	522	BE_EXPONENT_LEN	invalid exponent length for public exponent in keypair generation
0x020b	523	BE_HARDWARE	cryptographic hardware error
0x020c	524	BE_INPUT_DATA	invalid encoding format for input data
0x020d	525	BE_INPUT_LEN	invalid total length for input data
0x020e	526	BE_KEY_ALREADY_SET	the value of the key object has already been set by a call to <code>B_SetKeyInfo</code> or by a key generation
0x020f	527	BE_KEY_INFO	invalid format for the key information in the key object
0x0210	528	BE_KEY_LEN	invalid key length
0x0211	529	BE_KEY_NOT_SET	the key object has not been set by a call to <code>B_SetKeyInfo</code> or by a key generation
0x0212	530	BE_KEY_OBJ	invalid key object
0x0213	531	BE_KEY_OPERATION_UNKNOWN	unknown operation for a key info type
0x0214	532	BE_MEMORY_OBJ	invalid internal memory object
0x0215	533	BE_MODULUS_LEN	unsupported modulus length for a key or for algorithm parameters
0x0216	534	BE_NOT_INITIALIZED	algorithm is improperly initialized
0x0217	535	BE_NOT_SUPPORTED	the algorithm chooser does not support the type of key information in the key object for the specified algorithm
0x0218	536	BE_OUTPUT_LEN	the maximum size or the output buffer is too small to receive the output
0x0219	537	BE_OVER_32K	data block exceeds 32,767 bytes
0x021a	538	BE_RANDOM_NOT_INITIALIZED	the random algorithm has not been initialized by a call to <code>B_RandomInit</code>
0x021b	539	BE_RANDOM_OBJ	invalid algorithm object for the random algorithm
0x021c	540	BE_SIGNATURE	signature does not verify

Table A-1 **Crypto-C Error Types**

Hex	Decimal	Error Code	Description
0x021d	541	BE_WRONG_ALGORITHM_INFO	the required algorithm information is not in the algorithm object
0x021e	542	BE_WRONG_KEY_INFO	the required key information is not in the key object
0x021f	543	BE_INPUT_COUNT	Update called an invalid number of times for inputting data
0x0220	544	BE_OUTPUT_COUNT	Update called an invalid number of times for outputting data
0x0221	545	BE_METHOD_NOT_IN_CHOOSER	algorithm chooser doesn't contain the algorithm method for the algorithm specified by the previous call to <code>B_SetAlgorithmInfo</code>
0x0222	546	BE_KEY_WEAK	the key data supplied would generate a known weak key
0x0223	547	BE_EXPONENT_ONE	the value of the public exponent can not be 1
0x0224	548	BE_BAD_POINTER	invalid pointer
0x0225	549	BE_BAD_PASSPHRASE	invalid password
0x0226	550	BE_AM_DOMESTIC_ONLY	an attempt was made to call a function that is not available in the export version of Crypto-C
0x0227	551	BE_BAD_SEEDING	bad seeding was passed to an <code>AI_X931Random</code> object



# Platform-Specific Types and Constants

---

This appendix lists the platform-specific types and constants.

## Types

Crypto-C requires these platform-specific types: `POINTER`, `UINT2`, and `UINT4`. These can be found in the file `global.h`.

### POINTER

A `POINTER` value is a generic pointer to memory to which any other pointer can be cast.

Example:

```
typedef unsigned char *POINTER;
```

### UINT2

A `UINT2` value is a 16-bit unsigned integer.

---

## Types

---

Example:

```
typedef unsigned short int UINT2;
```

## UINT4

A `UINT4` value is a 32-bit unsigned integer.

Example:

```
typedef unsigned long int UINT4;
```

---

# Constants

Crypto-C requires one macro: `PROTO_LIST`.

`PROTO_LIST` indicates the form that C function prototypes are to take. If function prototypes specify the types of the arguments, then `PROTO_LIST` should be defined as:

```
#define PROTO_LIST(list) list
```

Otherwise `PROTO_LIST` should be defined as:

```
#define PROTO_LIST(list) ()
```

Crypto-C defines one string constant: `BSAFE_VERSION`:

```
extern char *BSAFE_VERSION;
```

`BSAFE_VERSION` is a null-terminated string constant that specifies the release of the Crypto-C library.



# References

- 
- FIPS PUB 46-1 National Bureau of Standards. *FIPS Publication 46-1: Data Encryption Standard*. January 1988.
- FIPS PUB 81 National Bureau of Standards. *FIPS Publication 81: DES Modes of Operation*. December 1980.
- FIPS PUB 180-1 National Institute of Standards and Technology. *FIPS Publication 180-1: Secure Hash Standard*. May 1993.
- FIPS PUB 186 National Institute of Standards and Technology. *FIPS Publication 186: Digital Signature Standard*. May 1994.
- P1363 Draft D1 IEEE. *Standard Specifications for Public Key Cryptography*. December 1997.
- RFC 1113 J. Linn. *RFC 1113: Privacy Enhancement for Internet Electronic Mail: Part I Message Encipherment and Authentication Procedures*. August 1989.
- RFC 1319 B. Kaliski. *The MD2 Message-Digest Algorithm*. April 1992.
- RFC 1321 R. Rivest. *The MD5 Message-Digest Algorithm*. April 1992.
- RFC 1423 D. Balenson. *RFC 1423: Privacy Enhancement for Internet Electronic Mail: Part III Algorithms, Modes, and Identifiers*. February 1993.
- X.208 CCITT. *Recommendation X.208: Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1)*. 1988.

- 
- X.209 CCITT. *Recommendation X.209: Specification of Abstract Syntax Notation One (ASN.1)*. 1988.
- X.509 CCITT. *Recommendation X.509: The Directory Authentication Framework*. 1988.
- X9.31 Draft *Digital signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA)*. December 1997.
- X9.44 Draft *Key management using reversible public key cryptography for the financial services industry*. January 1998.
- X9.52 Draft *Triple Data Encryption Algorithm Modes of Operation*. December 1997.
- X9.57 Draft ANSI. *Certificate Management*, N5-95, June 15, 1995.
- X9.62 Draft ANSI. *The Elliptic Curve Digital Signature Algorithm (ECDSA)*. August 29, 1997.
- X9.63 Draft *Public Key Cryptography for the Financial Services Industry: Elliptic Curve Key Agreement and Transport Protocols*. December 1997.
- [NIST91] NIST. *Special Publication 500-202: Stable Implementation Agreements for Open Systems Interconnection Protocols*. Version 5, Edition 1, Part 12. December 1991.
- S.C. Kothari. *Proceedings of CRYPTO 84: Generalized Linear Threshold Scheme*. 1984.

The following references are from RSA Data Security, Inc.'s Public-Key Cryptography Standards (PKCS) suite:

- PKCS #1 RSA Data Security, Inc. *PKCS #1: RSA Encryption Standard*. Version 1.5, November 1993.
- PKCS #3 RSA Data Security, Inc. *PKCS #3: Diffie-Hellman Key-Agreement Standard*. Version 1.4, November 1993.
- PKCS #5 RSA Data Security, Inc. *PKCS #5: Password-Based Encryption Standard*. Version 1.5, November 1993.
- PKCS #7 RSA Data Security, Inc. *PKCS #7: Cryptographic Message Syntax Standard*. Version 1.5, November 1993.
- PKCS #8 RSA Data Security, Inc. *PKCS #8: Private-Key Information Syntax Standard*. Version 1.2, November 1993.

PKCS documents are available by anonymous FTP from the host `ftp.rsa.com` in the files `pub/pkcs/pkcs*.ps`, or by sending electronic mail to `pkcs@rsa.com`.

---

# Index

---

## A

- algorithm chooser 10
- algorithm info types
  - AI\_BSSecretSharing 17
  - AI\_CBC\_IV8 19
  - AI\_DES\_CBC\_BSAFE1 20
  - AI\_DES\_CBC\_IV8 22
  - AI\_DES\_CBCPadBER 24
  - AI\_DES\_CBCPadIV8 26
  - AI\_DES\_CBCPadPEM 28
  - AI\_DES\_EDE3\_CBC\_IV8 30
  - AI\_DES\_EDE3\_CBCPadBER 32
  - AI\_DES\_EDE3\_CBCPadIV8 34
  - AI\_DESX\_CBC\_BSAFE1 36
  - AI\_DESX\_CBC\_IV8 38
  - AI\_DESX\_CBCPadBER 40
  - AI\_DESX\_CBCPadIV8 42
  - AI\_DHKeyAgree 44
  - AI\_DHKeyAgreeBER 46
  - AI\_DHPParamGen 48
  - AI\_DSA 49
  - AI\_DSAPKeyGen 51
  - AI\_DSAPParamGen 53
  - AI\_DSAPWithSHA1 54
  - AI\_DSAPWithSHA1BER 56
  - AI\_EC\_DHKeyAgree 63
  - AI\_EC\_DSA 65
  - AI\_EC\_DSAPWithDigest 67
  - AI\_EC\_ES 69
  - AI\_ECAcceleratorTable 58
  - AI\_ECBuildAcceleratorTable 59
  - AI\_ECBuildPubKeyAccelTable 61
  - AI\_ECKKeyGen 70
  - AI\_ECParameters 72
  - AI\_ECParamGen 73
  - AI\_ECPublic 76
  - AI\_FeedbackCipher 77
  - AI\_HMAC 82
  - AI\_HW\_RANDOM 84
  - AI\_HW\_Random 84
  - AI\_KeypairTokenGen 85
  - AI\_MAC 87
  - AI\_MD 88
  - AI\_MD2 89
  - AI\_MD2\_BER 90
  - AI\_MD2\_PEM 92
  - AI\_MD2Random 94
  - AI\_MD2WithDES\_CBCPad 95
  - AI\_MD2WithDES\_CBCPadBER 97
  - AI\_MD2WithRC2\_CBCPad 99
  - AI\_MD2WithRC2\_CBCPadBER 101
  - AI\_MD2WithRSAEncryption 103
  - AI\_MD2WithRSAEncryptionBER 105
  - AI\_MD5 107
  - AI\_MD5\_BER 108
  - AI\_MD5\_PEM 110
  - AI\_MD5Random 112
  - AI\_MD5WithDES\_CBCPad 113
  - AI\_MD5WithDES\_CBCPadBER 115
  - AI\_MD5WithRC2\_CBCPad 117
  - AI\_MD5WithRC2\_CBCPadBER 119
  - AI\_MD5WithRSAEncryption 121
  - AI\_MD5WithRSAEncryptionBER 123
  - AI\_MD5WithXOR 125
  - AI\_MD5WithXOR\_BER 127
  - AI\_PKCS\_OAEP\_RSAPrivate 129
  - AI\_PKCS\_OAEP\_RSAPrivateBER 133
  - AI\_PKCS\_OAEP\_RSAPublic 137
  - AI\_PKCS\_OAEP\_RSAPublicBER 141
  - AI\_PKCS\_OAEPRecode 146
  - AI\_PKCS\_OAEPRecodeBER 150
  - AI\_PKCS\_RSAPrivate 155
  - AI\_PKCS\_RSAPrivateBER 157
  - AI\_PKCS\_RSAPrivatePEM 159
  - AI\_PKCS\_RSAPublic 161
  - AI\_PKCS\_RSAPublicBER 163
  - AI\_PKCS\_RSAPublicPEM 165
  - AI\_RC2\_CBC 167
  - AI\_RC2\_CBC\_BSAFE1 169
  - AI\_RC2\_CBCPad 171
  - AI\_RC2\_CBCPadBER 173
  - AI\_RC2\_CBCPadPEM 175, 176
  - AI\_RC4 177
  - AI\_RC4\_BER 180
  - AI\_RC4WithMAC 181
  - AI\_RC4WithMAC\_BER 183
  - AI\_RC5\_CBC 185
  - AI\_RC5\_CBCPad 187

---

AI\_RC5\_CBCPadBER 189  
 AI\_RESET\_IV 191  
 AI\_RFC1113Recode 192  
 AI\_RSAKeyGen 193  
 AI\_RSAPrivate 195  
 AI\_RSAPrivateBSAFE1 197  
 AI\_RSAPublic 199  
 AI\_RSAPublicBSAFE1 201  
 AI\_RSAStrongKeyGen 203  
 AI\_SET\_OAEP\_RSAPrivate 205  
 AI\_SET\_OAEP\_RSAPublic 207  
 AI\_SHA1 209  
 AI\_SHA1\_BER 210  
 AI\_SHA1Random 212  
 AI\_SHA1WithDES\_CBCPad 213  
 AI\_SHA1WithDES\_CBCPadBER 215  
 AI\_SHA1WithRSAEncryption 217  
 AI\_SHA1WithRSAEncryptionBER 219  
 AI\_SignVerify 221, 223  
 AI\_SymKeyTokenGen 223  
 AI\_X92Random\_v0 227  
 AI\_X931Random 225  
 entry format 16  
 algorithm methods  
 AM\_CBC\_DECRYPT 80  
 AM\_CBC\_ENCRYPT 79  
 AM\_CBC\_INTER\_LEAVED\_DECRYPT 80  
 AM\_CBC\_INTER\_LEAVED\_ENCRYPT 80  
 AM\_CFB\_DECRYPT 80  
 AM\_CFB\_ENCRYPT 80  
 AM\_CFB\_PIPELINED\_DECRYPT 80  
 AM\_CFB\_PIPELINED\_ENCRYPT 80  
 AM\_DES\_CBC\_DECRYPT 20, 22, 24, 26, 28, 96,  
 97, 114, 115, 214, 215  
 AM\_DES\_CBC\_ENCRYPT 20, 22, 24, 26, 28, 96,  
 97, 114, 115, 214, 215  
 AM\_DES\_DECRYPT 78  
 AM\_DES\_EDE\_DECRYPT 79  
 AM\_DES\_EDE\_ENCRYPT 78  
 AM\_DES\_EDE3\_CBC\_DECRYPT 30, 33, 34  
 AM\_DES\_EDE3\_CBC\_ENCRYPT 30, 33, 34  
 AM\_DES\_ENCRYPT 78  
 AM\_DESX\_CBC\_DECRYPT 36, 38, 40, 42  
 AM\_DESX\_CBC\_ENCRYPT 36, 38, 40, 42  
 AM\_DESX\_DECRYPT 79  
 AM\_DESX\_ENCRYPT 78  
 AM\_DH\_KEY\_AGREE 45, 46  
 AM\_DH\_PARAM\_GEN 48  
 AM\_DSA\_KEY\_GEN 52  
 AM\_DSA\_KEY\_TOKEN\_GEN 86  
 AM\_DSA\_PARAM\_GEN 53  
 AM\_DSA\_SIGN 49, 54, 56  
 AM\_DSA\_VERIFY 49, 54, 56  
 AM\_ECB\_DECRYPT 80  
 AM\_ECB\_ENCRYPT 80  
 AM\_ECF2POLY\_BLD\_ACCEL\_TABLE 60  
 AM\_ECF2POLY\_BLD\_PUB\_KEY\_ACCEL\_TABLE  
 62  
 AM\_ECF2POLY\_DECRYPT 69  
 AM\_ECF2POLY\_DH\_KEY\_AGREE 64  
 AM\_ECF2POLY\_DSA\_SIGN 65, 67  
 AM\_ECF2POLY\_DSA\_VERIFY 65, 67  
 AM\_ECF2POLY\_ENCRYPT 69  
 AM\_ECF2POLY\_KEY\_GEN 71  
 AM\_ECF2POLY\_PARAM\_GEN 75  
 AM\_ECFP\_BLD\_ACCEL\_TABLE 60  
 AM\_ECFP\_BLD\_PUB\_KEY\_ACCEL\_TABLE 62  
 AM\_ECFP\_DECRYPT 69  
 AM\_ECFP\_DH\_KEY\_AGREE 64  
 AM\_ECFP\_DSA\_SIGN 65, 67  
 AM\_ECFP\_DSA\_VERIFY 65, 67  
 AM\_ECFP\_ENCRYPT 69  
 AM\_ECFP\_KEY\_GEN 71  
 AM\_ECFP\_PARAM\_GEN 75  
 AM\_HW\_RANDOM 84  
 AM\_MAC 87  
 AM\_MD 88  
 AM\_MD2 89, 90, 92, 96, 97, 100, 101, 103, 106,  
 121, 124, 217, 220  
 AM\_MD2\_RANDOM 94  
 AM\_MD5 107, 108, 110, 114, 115, 118, 119, 126,  
 127  
 AM\_MD5\_RANDOM 112, 126, 127  
 AM\_OFB\_DECRYPT 80  
 AM\_OFB\_ENCRYPT 80  
 AM\_OFB\_PIPELINED\_DECRYPT 80  
 AM\_OFB\_PIPELINED\_ENCRYPT 80  
 AM\_RC2\_CBC\_DECRYPT 100, 101, 118, 119,  
 168, 169, 172, 173, 175  
 AM\_RC2\_CBC\_ENCRYPT 100, 101, 118, 119,  
 168, 169, 172, 173, 175  
 AM\_RC2\_DECRYPT 79  
 AM\_RC2\_ENCRYPT 78  
 AM\_RC4\_DECRYPT 177, 180  
 AM\_RC4\_ENCRYPT 177, 180  
 AM\_RC4\_WITH\_MAC\_DECRYPT 182, 184  
 AM\_RC4\_WITH\_MAC\_ENCRYPT 182, 184  
 AM\_RC5\_64\_ENCRYPT 78  
 AM\_RC5\_64DECRYPT 79  
 AM\_RC5\_CBC\_DECRYPT 186, 188, 189  
 AM\_RC5\_CBC\_ENCRYPT 186, 188, 189  
 AM\_RC5\_DECRYPT 79  
 AM\_RC5\_ENCRYPT 78  
 AM\_RSA\_CRT\_DECRYPT 131, 136, 155, 158,  
 160, 196, 198, 205  
 AM\_RSA\_CRT\_DECRYPT\_BLIND 131, 136,  
 155, 158, 160, 196, 198, 205  
 AM\_RSA\_CRT\_ENCRYPT 103, 106, 121, 124,  
 155, 157, 160, 195, 198, 205, 217, 220  
 AM\_RSA\_CRT\_ENCRYPT\_BLIND 103, 106,

121, 124, 155, 157, 160, 195, 198, 205, 217, 220  
 AM\_RSA\_DECRYPT 103, 106, 121, 124, 161,  
 164, 165, 200, 202, 207, 217, 220  
 AM\_RSA\_ENCRYPT 103, 106, 121, 124, 139,  
 161, 164, 165, 200, 202, 207, 217, 220  
 AM\_RSA\_KEY\_GEN 194  
 AM\_RSA\_KEY\_TOKEN\_GEN 86  
 AM\_RSA\_STRONG\_KEY\_GEN 204  
 AM\_SHA 54, 68, 82, 131, 136, 139, 148, 153,  
 209, 210, 214, 215  
 AM\_SHA\_RANDOM 228  
 AM\_SHA1 56  
 AM\_TOKEN\_DES\_CBC\_DECRYPT 23  
 AM\_TOKEN\_DES\_CBC\_ENCRYPT 23  
 AM\_TOKEN\_DES\_EDE3\_CBC\_DECRYPT 31  
 AM\_TOKEN\_DES\_EDE3\_CBC\_ENCRYPT 31  
 AM\_TOKEN\_DSA\_SIGN 50  
 AM\_TOKEN\_DSA\_VERIFY 50  
 AM\_TOKEN\_RC2\_CBC\_DECRYPT 168  
 AM\_TOKEN\_RC2\_CBC\_ENCRYPT 168  
 AM\_TOKEN\_RC4\_DECRYPT 178  
 AM\_TOKEN\_RC4\_ENCRYPT 178  
 AM\_TOKEN\_RC4\_WITH\_MAC\_DECRYPT 182  
 AM\_TOKEN\_RC4\_WITH\_MAC\_ENCRYPT 182  
 AM\_TOKEN\_RC5\_CBC\_DECRYPT 186  
 AM\_TOKEN\_RC5\_CBC\_ENCRYPT 186  
 AM\_TOKEN\_RSA\_CRT\_DECRYPT 196  
 AM\_TOKEN\_RSA\_CRT\_ENCRYPT 196  
 AM\_TOKEN\_RSA\_DECRYPT 200  
 AM\_TOKEN\_RSA\_ENCRYPT 200  
 AM\_TOKEN\_RSA\_PUB\_DECRYPT 200  
 AM\_X931\_RANDOM 226  
 algorithm object 8  
 algorithms  
   3DES 30, 32, 34, 36, 77  
   Bloom/Shamir 17  
   DES 20, 22, 24, 26, 28, 77  
   DESX 40, 77  
   Diffie-Hellman 44, 46, 48  
   DSA 49, 51, 53, 54, 56  
   EC Diffie-Hellman 63  
   ECAES 69  
   ECDSA 65, 67  
   elliptic curve 58, 59, 61, 76  
     key pair 70  
     parameters 72, 73  
   HMAC 82  
   MD 88  
   MD2 89, 90, 92  
   MD5 107, 108, 110  
   PBE  
     MD2 with RC2 101  
     MD2 with RSA 103, 105  
     MD5 with DES 115  
   RC2 77, 169  
   RC5 77  
   RSA 121, 123  
     private key 155, 157, 195, 197, 205  
     public 207  
     public key 161, 163, 165, 199, 201  
   SHA-1 209, 210  
   SHA-1 Random 227  
 ASCII to binary 192  
**B**  
 BER encoding 24, 40, 46, 48, 56, 90, 101, 105, 108,  
 115, 123, 157, 163, 210  
 BHAPI methods  
   AM\_TOKEN\_DES\_CBC\_DECRYPT 23  
   AM\_TOKEN\_DES\_CBC\_ENCRYPT 23  
   AM\_TOKEN\_DES\_EDE3\_CBC\_DECRYPT 31  
   AM\_TOKEN\_DES\_EDE3\_CBC\_ENCRYPT 31  
   AM\_TOKEN\_DSA\_SIGN 50  
   AM\_TOKEN\_DSA\_VERIFY 50  
   AM\_TOKEN\_RC2\_CBC\_DECRYPT 168  
   AM\_TOKEN\_RC2\_CBC\_ENCRYPT 168  
   AM\_TOKEN\_RC4\_DECRYPT 178  
   AM\_TOKEN\_RC4\_ENCRYPT 178  
   AM\_TOKEN\_RC4\_WITH\_MAC\_DECRYPT 182  
   AM\_TOKEN\_RC4\_WITH\_MAC\_ENCRYPT 182  
   AM\_TOKEN\_RC5\_CBC\_DECRYPT 186  
   AM\_TOKEN\_RC5\_CBC\_ENCRYPT 186  
   AM\_TOKEN\_RSA\_CRT\_DECRYPT 196  
   AM\_TOKEN\_RSA\_CRT\_ENCRYPT 196  
   AM\_TOKEN\_RSA\_DECRYPT 200  
   AM\_TOKEN\_RSA\_ENCRYPT 200  
   AM\_TOKEN\_RSA\_PUB\_DECRYPT 200  
 binary to ASCII 192  
 BSAFE\_VERSION 337  
**F**  
 functions  
   B\_BuildTableFinal 270  
   B\_BuildTableGetBufSize 271  
   B\_BuildTableInit 272  
   B\_CreateAlgorithmObject 273  
   B\_CreateSessionChooser 275  
   B\_DecodeDigestInfo 276  
   B\_DecodeFinal 277  
   B\_DecodeInit 278  
   B\_DecodeUpdate 279  
   B\_DecryptFinal 280  
   B\_DecryptInit 281  
   B\_DecryptUpdate 282  
   B\_DestroyAlgorithmObject 283  
   B\_DestroyKeyObject 284  
   B\_DigestFinal 285  
   B\_DigestInit 286  
   B\_DigestUpdate 287

---

B\_EncodeDigestInfo 288  
 B\_EncodeFinal 289  
 B\_EncodeInit 290  
 B\_EncodeUpdate 291  
 B\_EncryptFinal 292  
 B\_EncryptInit 293  
 B\_EncryptUpdate 294  
 B\_FreeSessionChooser 295  
 B\_GenerateInit 296  
 B\_GenerateKeypair 297  
 B\_GenerateParameters 298  
 B\_GenerateRandomBytes 299  
 B\_GetAlgorithmInfo 300  
 B\_GetExtendedErrorInfo 301  
 B\_GetKeyExtendedErrorInfo 302  
 B\_GetKeyInfo 303  
 B\_IntegerBits 304  
 B\_KeyAgreeInit 305  
 B\_KeyAgreePhase1 306  
 B\_KeyAgreePhase2 307  
 B\_RandomInit 308  
 B\_RandomUpdate 309  
 B\_SetAlgorithmInfo 310  
 B\_SetKeyInfo 311  
 B\_SignFinal 312  
 B\_SignInit 313  
 B\_SignUpdate 314  
 B\_SymmetricKeyGenerate 315  
 B\_SymmetricKeyGenerateInit 316  
 B\_VerifyFinal 317  
 B\_VerifyInit 318  
 B\_VerifyUpdate 319  
 T\_free 320  
 T\_malloc 321  
 T\_memcmp 322  
 T\_memcpy 323  
 T\_memmove 324  
 T\_memset 325  
 T\_realloc 326  
 T\_strcmp 327  
 T\_strcpy 328  
 T\_strlen 329

**I**  
 initialization vector  
   resetting 19, 191

**K**  
 key info types  
   KI\_24Byte 232  
   KI\_8Byte 231  
   KI\_DES\_BSAFE1 236  
   KI\_DES24Strong 235  
   KI\_DES8 233  
   KI\_DES8Strong 234  
   KI\_DESX 237  
   KI\_DESX\_BSAFE1 238  
   KI\_DSAPrivate 239  
   KI\_DSAPrivateBER 241  
   KI\_DSAPrivateX957BER 242  
   KI\_DSAPublic 243  
   KI\_DSAPublicBER 245  
   KI\_DSAPublicX957BER 246  
   KI\_ECPrivate 247, 256  
   KI\_ECPrivateComponent 248  
   KI\_ECPublic 249  
   KI\_ECPublicComponent 250  
   KI\_ExtendedToken 23, 31, 168, 178, 182, 186,  
     251  
   KI\_Item 253  
   KI\_KeypairToken 50, 196, 200, 254  
   KI\_PKCS\_RSAPrivate 256  
   KI\_PKCS\_RSAPrivateBER 257  
   KI\_RC2\_BSAFE1 258  
   KI\_RC2WithBSAFE1Params 259  
   KI\_RSA\_CRT 260  
   KI\_RSAPrivate 261  
   KI\_RSAPrivateBSAFE1 263  
   KI\_RSAPublic 264  
   KI\_RSAPublicBER 265  
   KI\_RSAPublicBSAFE1 266  
   KI\_Token 23, 31, 50, 168, 178, 182, 186, 196, 200,  
     267

**P**  
 PEM encoding 28, 92, 110, 165  
 POINTER 335  
 PROTO\_LIST 337

**S**  
 standards  
   FIPS 186 54, 227  
   FIPS PUB 180-1 209  
   FIPS PUB 186 49, 51, 53, 56  
   FIPS PUB 46-1 22, 24, 26, 28  
   FIPS PUB 81 22, 26, 28  
   NIST 24  
   OAEP 205, 207  
   P1363 73  
   PKCS #1 103, 105, 121, 123, 155, 157, 161, 163,  
     165  
   PKCS #3 44, 46  
   PKCS #5 24, 26, 32, 115  
   PKCS #8 241  
   RFC 1113 192  
   RFC 1319 89, 90, 92  
   RFC 1321 108, 110  
   RFC 1421 192

---

RFC 1423 28, 110, 165  
SET 82, 205, 207  
X9.30 245  
X9.31 227  
X9.52 73, 77  
X9.57 54, 56, 242, 246  
X9.62 59, 61, 65, 67  
X9.63 63, 69  
X9.66 227

structures

A\_DESX\_KEY 237  
A\_DH\_KEY\_AGREE\_PARAMS 44  
A\_DH\_PARAM\_GEN\_PARAMS 48  
A\_DSA\_PARAMS 51, 239, 243  
A\_DSA\_PRIVATE\_KEY 239  
A\_DSA\_PUBLIC\_KEY 243  
A\_EC\_PARAMS 59, 63, 70, 72  
A\_EC\_PRIVATE\_KEY 247  
A\_EC\_PUBLIC\_KEY 61, 76, 249  
A\_KEYPAIR\_DEFINDER 85, 254  
A\_PKCS\_OAEP\_PARAMS 130, 138, 147  
A\_PKCS\_RSA\_PRIVATE\_KEY 256  
A\_RC2\_CBC\_PARAMS 167, 171  
A\_RC2\_PARAMS 79  
A\_RC5\_CBC\_PARAMS 185, 187  
A\_RC5\_PARAMS 79  
A\_RSA\_CRT\_KEY 260  
A\_RSA\_KEY 261, 264  
A\_RSA\_KEY\_GEN\_PARAMS 193, 203  
A\_SHA\_RANDOM\_PARAMS 227  
A\_SURRENDER\_CTX 12  
A\_SYMMETRIC\_KEY\_DEFINDER 251  
A\_SYMMETRIC\_KEY\_SPECIFIER 223  
A\_X509\_ATTRIB\_INFO 251  
A\_X509\_KEYPAIR\_ATTRIB\_INFO 254  
A\_X931\_RANDOM\_PARAMS 225  
B\_BLK\_CIPHER\_W\_FEEDBACK\_PARAMS 77  
B\_BSAFE1\_ENCRYPTION\_PARAMS 20, 36,  
169, 197, 201  
B\_CFB\_PARAMS 80  
B\_DIGEST\_SPECIFIER 67, 82  
B\_DSA\_PARAM\_GEN\_PARAMS 53  
B\_EC\_PARAM\_GEN\_PARAMS 73  
B\_EC\_PARAMS 59, 61, 63, 70  
B\_MAC\_PARAMS 87  
B\_PBE\_PARAMS 95, 113, 125, 213  
B\_RC2\_BSAFE1\_PARAMS\_KEY 259  
B\_RC2\_PBE\_PARAMS 99, 118  
B\_RC4\_WITH\_MAC\_PARAMS 181  
B\_SECRET\_SHARING\_PARAMS 17  
B\_SIGN\_VERIFY\_PARAMS 221  
ITEM 14  
KI\_EXTENDED\_TOKEN\_INFO 251  
KI\_KEYPAIR\_TOKEN\_INFO 254  
KI\_TOKEN\_INFO 267

surrender function 12

**U**

UINT2 335  
UINT4 336

