Microsoft Windows Vista Cryptographic Primitives Library (bcrypt.dll) Security Policy Document

Microsoft Windows Vista SP1 Operating System

FIPS 140-2 Security Policy Document

This document specifies the security policy for the Microsoft Windows Cryptographic Primitives Library (BCRYPT.DLL) as described in FIPS PUB 140-2.

April 14, 2008

Document Version: 1.3

1 Cryptographic Module Specification

The Microsoft Windows Cryptographic Primitives Library is a general purpose, software-based, cryptographic module. The primitive provider functionality is offered through one cryptographic module, BCRYPT.DLL (version 6.0.6001.22202), subject to FIPS-140-2 validation. BCRYPT.DLL provides cryptographic services, through its documented interfaces, to Windows Vista components and applications running on Windows Vista.

The cryptographic module, BCRYPT.DLL, encapsulates several different cryptographic algorithms in an easy-to-use cryptographic module accessible via the Microsoft CNG (Cryptography, Next Generation) API. It can be dynamically linked into applications by software developers to permit the use of general-purpose FIPS 140-2 Level 1 compliant cryptography.

1.1 Cryptographic Boundary

The Windows Vista BCRYPT.DLL consists of a dynamically-linked library (DLL). The cryptographic boundary for BCRYPT.DLL is defined as the enclosure of the computer system, on which BCRYPT.DLL is to be executed. The physical configuration of BCRYPT.DLL, as defined in FIPS-140-2, is multi-chip standalone.

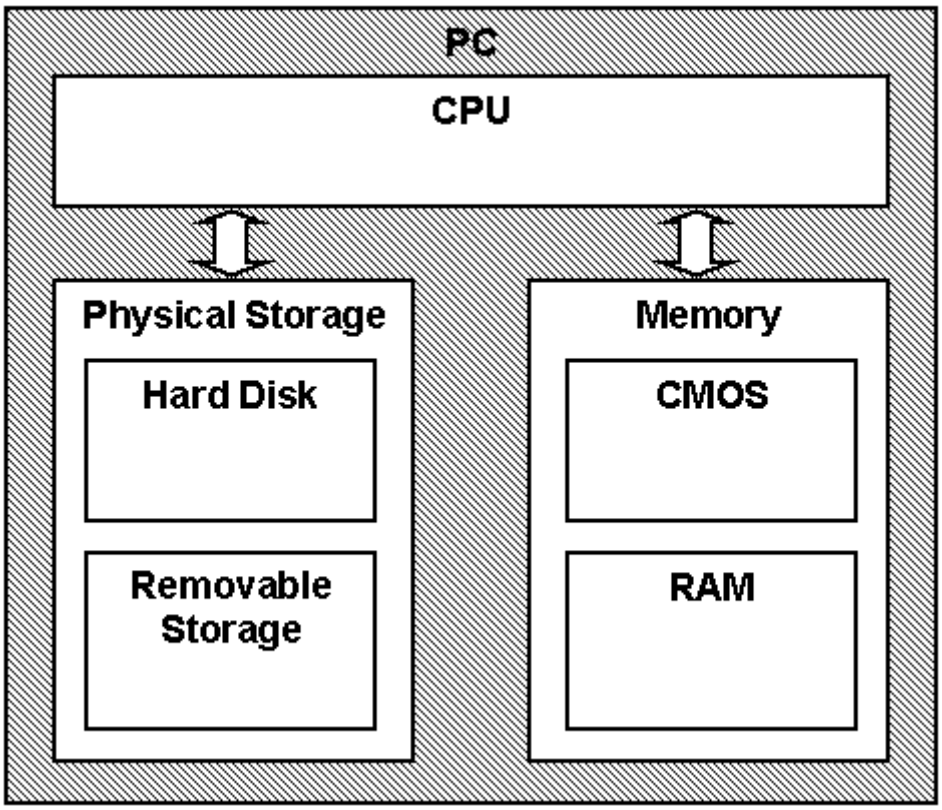
2 Security Policy

BCRYPT.DLL operates under several rules that encapsulate its security policy.

- BCRYPT.DLL is supported on Windows Vista Service Pack 1.
- BCRYPT.DLL operates in FIPS mode of operation only when used with the FIPS approved version of CI.DLL (FIPS 140-2 Cert. #980) operating in FIPS mode
- Windows Vista is an operating system supporting a "single user" mode where there is only one interactive user during a logon session.
- BCRYPT.DLL is only in its Approved mode of operation when Windows is booted normally, meaning Debug mode is disabled and Driver Signing enforcement is enabled.
- All users assume either the User or Cryptographic Officer roles.
- BCRYPT.DLL provides no authentication of users. Roles are assumed implicitly. The authentication provided by the Windows Vista operating system is not in the scope of the validation.
- All cryptographic services implemented within BCRYPT.DLL are available to the User and Cryptographic Officer roles.
- BCRYPT.DLL implements the following FIPS-140-2 Approved algorithms.
    - SHA-1, SHA-256, SHA-384, SHA-512 hash (Cert. #753)
    - SHA-1, SHA-256, SHA-384, SHA-512 HMAC (Cert. #412)
    - Triple-DES (2 key and 3 key) in ECB, CBC, and CFB with 8-bit feedback modes (Cert. #656)
    - AES-128, AES-192, AES-256 in ECB, CBC, and CFB with 8-bit feedback mode (Cert. #739)
    - AES-128, AES-192 and AES-256 in CCM (Cert. #756)
    - RSA (RSASSA-PKCS1-v1_5 and RSASSA-PSS) digital signatures (Cert. #357) and X9.31 RSA key-pair generation (Cert. #353).
    - DSA (Cert. #283)
    - ECDSA with the following NIST curves: P-256, P-384, P-521 (Cert. #82).
    - SP800-90 AES-256 based counter mode random number generation algorithm (Vendor-Affirmed)
    - FIPS 186-2 DSA PRNG (Cert. #435).
- BCRYPT.DLL supports the following non-Approved algorithms allowed for use in FIPS mode.
    - Diffie-Hellman (DH) secret agreement (key agreement; key establishment methodology provides between 80 and 150 bits of encryption strength; non-compliant less than 80-bits of encryption strength).

    - ECDH with the following NIST curves: P-256, P-384, P-521 (key agreement; key establishment methodology provides between 128 and 256 bits of encryption strength)
    - RSA (key wrapping; key establishment methodology provides between 80 and 150 bits of encryption strength; non-compliant less than 80-bits of encryption strength).
    - TLS
    - SP800-90 Dual-EC DRBG random generator algorithm (non-compliant) – Output can be used for generation of initialization vectors
- BCRYPT.DLL also supports the following non FIPS 140-2 approved algorithms, though these algorithms may not be used when operating the module in a FIPS compliant manner.
    - AES-128, AES-192 and AES-256 in GCM mode (non-compliant)
    - AES-128, AES-192 and AES-256 in GMAC message authentication mode (non-compliant)
    - RC2, RC4, MD2, MD4, MD5, HMAC MD5[1].
    - DES in ECB, CBC, and CFB with 8-bit feedback
    - IKEv1 Key Derivation Functions

The following diagram illustrates the master components of the BCRYPT.DLL module



BCRYPT.DLL was tested using the following machine configurations:

x86	Microsoft Windows Vista Ultimate Edition SP1 (x86 version) – Dell SC430 (Intel Pentium D 2.8GHz)
x64	Microsoft Windows Vista Ultimate Edition SP1 (x64 version) – Dell SC430 (Intel Pentium D 2.8GHz)

[1] Applications may not use any of these non-FIPS algorithms if they need to be FIPS compliant. To operate the module in a FIPS compliant manner, applications must only use FIPS-approved algorithms.

3 Cryptographic Module Ports and Interfaces

3.1 Ports and Interfaces

3.1.1 Export Functions

The following list contains the functions exported by BCRYPT.DLL to its callers.

- BCryptCloseAlgorithmProvider
- BCryptCreateHash
- BCryptDecrypt
- BCryptDeriveKey
- BCryptDestroyHash
- BCryptDestroyKey
- BCryptDestroySecret
- BCryptDuplicateHash
- BCryptDuplicateKey
- BCryptEncrypt
- BCryptExportKey
- BCryptFinalizeKeyPair
- BCryptFinishHash
- BCryptFreeBuffer
- BCryptGenerateKeyPair
- BCryptGenerateSymmetricKey
- BCryptGenRandom
- BCryptGetProperty
- BCryptHashData
- BCryptImportKey
- BCryptImportKeyPair
- BCryptOpenAlgorithmProvider
- BCryptSecretAgreement
- BCryptSetProperty
- BCryptSignHash
- BCryptVerifySignature

Additionally, BCRYPT.DLL exports crypto configuration functions. They are described in a separate section below for informational purposes.

3.1.2 Data Input and Output Interfaces

The Data Input Interface for BCRYPT.DLL consists of the BCRYPT export functions. Data and options are passed to the interface as input parameters to the BCRYPT export functions. Data Input is kept separate from Control Input by passing Data Input in separate parameters from Control Input.

The Data Output Interface for BCRYPT.DLL also consists of the BCRYPT export functions.

3.1.3 Control Input Interface

The Control Input Interface for BCRYPT.DLL also consists of the BCRYPT export functions. Options for control operations are passed as input parameters to the BCRYPT export functions.

3.1.4 Status Output Interface

The Status Output Interface for BCRYPT.DLL also consists of the BCRYPT export functions. For each function, the status information is returned to the caller as the return value from the function.

3.2 Cryptographic Bypass

Cryptographic bypass is not supported by BCRYPT.DLL.

4 Roles and Authentication

4.1 Roles

BCRYPT.DLL provides User and Cryptographic Officer roles (as defined in FIPS 140-2). These roles share all the services implemented in the cryptographic module.
When an application requests the crypto module to generate keys for a user, the keys are generated, used, and deleted as requested by applications. There are no implicit keys associated with a user. Each user may have numerous keys, and each user's keys are separate from other users' keys.

4.2 Maintenance Roles

Maintenance roles are not supported by BCRYPT.DLL.

4.3 Operator Authentication

The module does not provide authentication. Roles are implicitly assumed based on the services that are executed.

The OS on which BCRYPT.DLL executes (Microsoft Windows Vista) does authenticate users.
Microsoft Windows Vista requires authentication from the trusted control base (TCB) before a user is able to access system services. Once a user is authenticated from the TCB, a process is created bearing the Authenticated User's security token for identification purpose. All subsequent processes and threads created by that Authenticated User are implicitly assigned the parent's (thus the Authenticated User's) security token.

5 Services

The following list contains all services available to an operator. All services are accessible to both the User and Crypto Officer roles.

5.1 Algorithm Providers and Properties

5.1.1 BCryptOpenAlgorithmProvider

```
NTSTATUS WINAPI BCryptOpenAlgorithmProvider(
        BCRYPT_ALG_HANDLE   *phAlgorithm,
        LPCWSTR pszAlgId,
        LPCWSTR pszImplementation,
        ULONG   dwFlags);
```

The BCryptOpenAlgorithmProvider() function has four parameters: algorithm handle output to the opened algorithm provider, desired algorithm ID input, an optional specific provider name input, and optional flags. This function loads and initializes a CNG provider for a given algorithm, and returns a handle to the opened algorithm provider on success. See http://msdn.microsoft.com for CNG providers. Unless the calling function specifies the name of the provider, the default provider is used. The default provider is the first provider listed for a given algorithm. The calling function must pass the BCRYPT_ALG_HANDLE_HMAC_FLAG flag in order to use an HMAC function with a hash algorithm.

5.1.2 BCryptCloseAlgorithmProvider

```
NTSTATUS WINAPI BCryptCloseAlgorithmProvider(
        BCRYPT_ALG_HANDLE   hAlgorithm,
        ULONG   dwFlags);
```

This function closes an algorithm provider handle opened by a call to BCryptOpenAlgorithmProvider() function.

5.1.3 BCryptSetProperty

```
NTSTATUS WINAPI BCryptSetProperty(
        BCRYPT_HANDLE   hObject,
        LPCWSTR pszProperty,
        PUCHAR   pbInput,
        ULONG   cbInput,
        ULONG   dwFlags);
```

The BCryptSetProperty() function sets the value of a named property for a CNG object, e.g., a cryptographic key. The CNG object is referenced by a handle, the property name is a NULL terminated string, and the value of the property is a length-specified byte string.

5.1.4 BCryptGetProperty

```
NTSTATUS WINAPI BCryptGetProperty(
        BCRYPT_HANDLE   hObject,
        LPCWSTR pszProperty,
        PUCHAR   pbOutput,
        ULONG   cbOutput,
        ULONG   *pcbResult,
        ULONG   dwFlags);
```

The BCryptGetProperty() function retrieves the value of a named property for a CNG object, e.g., a cryptographic key. The CNG object is referenced by a handle, the property name is a NULL terminated string, and the value of the property is a length-specified byte string.

5.1.5 BCryptFreeBuffer

```
VOID WINAPI BCryptFreeBuffer(
        PVOID   pvBuffer);
```

Some of the CNG functions allocate memory on caller's behalf. The BCryptFreeBuffer() function frees memory that was allocated by such a CNG function.

5.2 Random Number Generation

5.2.1 BCryptGenRandom

```
NTSTATUS WINAPI BCryptGenRandom(
        BCRYPT_ALG_HANDLE   hAlgorithm,
        PUCHAR  pbBuffer,
        ULONG   cbBuffer,
        ULONG   dwFlags);
```

The BCryptGenRandom() function fills a buffer with random bytes. There are two random number generation algorithms:

- BCRYPT_RNG_ALGORITHM. This is the AES-256 counter mode based random generator as defined in SP800-90.
- BCRYPT_RNG_FIPS186_DSA_ALGORITHM. This is the random number generator required by the DSA algorithm as defined in FIPS 186-2.
- BCRYPT_RNG_DUAL_EC_ALGORITHM. This is the non-compliant Dual-EC DRBG based random generator as defined in SP800-90. The output from calls to this PRNG cannot be used for keys; however, it is available for generation of initialization vectors per FIPS 140-2.

When BCRYPT_RNG_USE_ENTROPY_IN_BUFFER is specified in the *dwFlags* parameter, this function will use the number in the *pbBuffer* buffer as additional entropy for the random number. If this flag is not specified, this function will use a random number for the entropy.

During the function initialization, a seed, to which SHA-1 is applied to create the output random, is created based on the collection of all the following data.

- The process ID of the current process requesting random data

- The thread ID of the current thread within the process requesting random data
- A 32-bit tick count since the system boot
- The current local date and time
- The current system time of day information consisting of the boot time, current time, time zone bias, time zone ID, boot time bias, and sleep time bias
- The current hardware-platform-dependent high-resolution performance-counter value
- The information about the system's current usage of both physical and virtual memory, and page file, Zero Page Count, Free Page Count, Modified Page Count, Modified No Write Page Count, Bad Page Count, Page Count By Priority, Repurposed Pages By Priority
- The system device information consisting of Number Of Disks, Number Of Floppies, Number Of CD Roms, Number Of Tapes, Number Of Serial Ports, Number Of Parallel Ports
- The local disk information including the numbers of sectors per cluster, bytes per sector, free clusters, and clusters that are available to the user associated with the calling thread
- A hash of the environment block for the current process
- Some hardware CPU-specific cycle counters
- The system file cache information consisting of Current Size, Peak Size, Page Fault Count, Minimum Working Set, Maximum Working Set, Current Size Including Transition In Pages, Peak Size Including Transition In Pages, Transition Repurpose Count, Flags
- The system processor power information consisting of Current Frequency, Thermal Limit Frequency, Constant Throttle Frequency, Degraded Throttle Frequency, Last Busy Frequency, Last C3 Frequency, Last Adjusted Busy Frequency, Processor Min Throttle, Processor Max Throttle, Number Of Frequencies, Promotion Count, Demotion Count, Error Count, Retry Count, Current Frequency Time, Current Processor Time, Current Processor Idle Time, Last Processor Time, Last Processor Idle Time
- The system page file information consisting of Next Entry Offset, Total Size, Total In-Use, Peak Usage, Page File Name
- The system processor idle information consisting of Idle Time
- The system processor performance information consisting of Idle Process Time, Io Read Transfer Count, Io Write Transfer Count, Io Other Transfer Count, Io Read Operation Count, Io Write Operation Count, Io Other Operation Count, Available Pages, Committed Pages, Commit Limit, Peak Commitment, Page Fault Count, Copy On Write Count, Transition Count, Cache Transition Count, Demand Zero Count, Page Read Count, Page Read Io Count, Cache Read Count, Cache Io Count, Dirty Pages Write Count, Dirty Write Io Count, Mapped Pages Write Count, Mapped Write Io Count, Paged Pool Pages, Non Paged Pool Pages, Paged Pool Allocated space, Paged Pool Free space, Non Paged Pool Allocated space, Non Paged Pool Free space, Free System page table entry, Resident System Code Page, Total System Driver Pages, Total System Code Pages, Non Paged Pool Look aside Hits, Paged Pool Lookaside Hits, Available Paged Pool Pages, Resident System Cache Page, Resident Paged Pool Page, Resident System Driver Page, Cache manager Fast Read with No Wait, Cache manager Fast Read with Wait, Cache manager Fast Read Resource Missed, Cache manager Fast Read Not Possible, Cache manager Fast Memory Descriptor List Read with No Wait, Cache manager Fast Memory Descriptor List Read with Wait, Cache manager Fast Memory Descriptor List Read Resource Missed, Cache manager Fast Memory Descriptor List Read Not Possible, Cache manager Map Data with No Wait, Cache manager Map Data with Wait, Cache manager Map Data with No Wait Miss, Cache manager Map Data Wait Miss, Cache manager Pin-Mapped Data Count, Cache manager Pin-Read with No Wait, Cache manager Pin Read with Wait, Cache manager Pin-Read with No Wait Miss, Cache manager Pin-Read Wait Miss, Cache manager Copy-Read with No Wait, Cache manager Copy-Read with Wait, Cache manager Copy-Read with No Wait Miss, Cache manager Copy-Read with Wait Miss, Cache manager Memory Descriptor List Read with No Wait, Cache manager Memory Descriptor List Read with Wait, Cache manager Memory Descriptor List Read with No Wait Miss, Cache manager Memory Descriptor List Read with Wait Miss, Cache manager Read Ahead IOs, Cache manager Lazy-Write IOs, Cache manager Lazy-Write Pages, Cache manager Data Flushes, Cache manager

Data Pages, Context Switches, First Level Translation buffer Fills, Second Level Translation buffer Fills, and System Calls
- The system exception information consisting of Alignment Fix up Count, Exception Dispatch Count, Floating Emulation Count, and Byte Word Emulation Count
- The system look-aside information consisting of Current Depth, Maximum Depth, Total Allocates, Allocate Misses, Total Frees, Free Misses, Type, Tag, and Size
- The system processor performance information consisting of Idle Time, Kernel Time, User Time, Deferred Process Call Time, Interrupt Time Interrupt Count
- The system interrupt information consisting of context switches, deferred procedure call count, deferred procedure call rate, time increment, deferred procedure call bypass count, and asynchronous procedure call bypass count
- The system process information consisting of Next Entry Offset, Number Of Threads, Working Set Private Size, Create Time, User Time, Kernel Time, Image Name, Base Priority, Unique Process Id, Inherited From Unique Process Id, Handle Count, Session Id, Unique Process Key, Peak Virtual Size, Virtual Size, Page Fault Count, Peak Working Set Size, Working Set Size, Quota Peak Paged Pool Usage, Quota Paged Pool Usage, Quota Peak Non Paged Pool Usage, Quota Non Paged Pool Usage, Pagefile Usage, Peak Pagefile Usage, Private Page Count, Read Operation Count, Write Operation Count, Other Operation Count, Read Transfer Count, Write Transfer Count, Other Transfer Count
- Random data from the hardware based RNG on the Trusted Platform Module (TPM)

5.3 Key and Key-Pair Generation

5.3.1 BCryptGenerateSymmetricKey

```
NTSTATUS WINAPI BCryptGenerateSymmetricKey(
        BCRYPT_ALG_HANDLE   hAlgorithm,
        BCRYPT_KEY_HANDLE   *phKey,
        PUCHAR   pbKeyObject,
        ULONG   cbKeyObject,
        PUCHAR   pbSecret,
        ULONG   cbSecret,
        ULONG   dwFlags);
```

The BCryptGenerateSymmetricKey() function generates a symmetric key object for use with a symmetric encryption algorithm from a supplied *cbSecret* bytes long key value provided in the *pbSecret* memory location. The calling application must specify a handle to the algorithm provider opened with the BCryptOpenAlgorithmProvider() function. The algorithm specified when the provider was opened must support symmetric key encryption.

5.3.2 BCryptGenerateKeyPair

```
NTSTATUS WINAPI BCryptGenerateKeyPair(
        BCRYPT_ALG_HANDLE   hAlgorithm,
        BCRYPT_KEY_HANDLE   *phKey,
        ULONG   dwLength,
        ULONG   dwFlags);
```

The BCryptGenerateKeyPair() function creates a public/private key pair object without any cryptographic keys in it. After creating such an empty key pair object using this function, call the BCryptSetProperty() function to set its properties. The key pair can be used only after BCryptFinalizeKeyPair() function is called.

5.3.3 BCryptFinalizeKeyPair

```
NTSTATUS WINAPI BCryptFinalizeKeyPair(
        BCRYPT_KEY_HANDLE   hKey,
        ULONG   dwFlags);
```

The BCryptFinalizeKeyPair() function completes a public/private key pair import or generation. The key pair cannot be used until this function has been called. After this function has been called, the BCryptSetProperty() function can no longer be used for this key pair.

5.3.4 BCryptDuplicateKey

```
NTSTATUS WINAPI BCryptDuplicateKey(
        BCRYPT_KEY_HANDLE   hKey,
        BCRYPT_KEY_HANDLE   *phNewKey,
        PUCHAR   pbKeyObject,
        ULONG   cbKeyObject,
        ULONG   dwFlags);
```

The BCryptDuplicateKey() function creates a duplicate of a symmetric key object.

5.3.5 BCryptDestroyKey

```
NTSTATUS WINAPI BCryptDestroyKey(
        BCRYPT_KEY_HANDLE   hKey);
```

The BCryptDestroyKey() function destroys a key.

5.4 Key Entry and Output

5.4.1 BCryptImportKey

```
NTSTATUS WINAPI BCryptImportKey(
        BCRYPT_ALG_HANDLE hAlgorithm,
        BCRYPT_KEY_HANDLE hImportKey,
        LPCWSTR pszBlobType,
        BCRYPT_KEY_HANDLE *phKey,
        PUCHAR   pbKeyObject,
        ULONG   cbKeyObject,
        PUCHAR   pbInput,
        ULONG   cbInput,
        ULONG   dwFlags);
```

The BCryptImportKey() function imports a symmetric key from a key blob.

hAlgorithm [in] is the handle of the algorithm provider to import the key. This handle is obtained by calling the BCryptOpenAlgorithmProvider function.
hImportKey [in, out] is not currently used and should be NULL.
pszBlobType [in] is a null-terminated Unicode string that contains an identifier that specifies the type of BLOB that is contained in the *pbInput* buffer. *pszBlobType* can be one of BCRYPT_KEY_DATA_BLOB and BCRYPT_OPAQUE_KEY_BLOB.
phKey [out] is a pointer to a BCRYPT_KEY_HANDLE that receives the handle of the imported key that is used in subsequent functions that require a key, such as BCryptEncrypt. This handle must be released when it is no longer needed by passing it to the BCryptDestroyKey function.
pbKeyObject [out] is a pointer to a buffer that receives the imported key object. The *cbKeyObject* parameter contains the size of this buffer. The required size of this buffer can be obtained by calling the BCryptGetProperty function to get the BCRYPT_OBJECT_LENGTH property. This will provide the size of the key object for the specified algorithm. This memory can only be freed after the *phKey* key handle is destroyed.
cbKeyObject [in] is the size, in bytes, of the pbKeyObject buffer.
pbInput [in] is the address of a buffer that contains the key BLOB to import.
The *cbInput* parameter contains the size of this buffer.
The *pszBlobType* parameter specifies the type of key BLOB this buffer contains.
cbInput [in] is the size, in bytes, of the pbInput buffer.

dwFlags [in] is a set of flags that modify the behavior of this function. No flags are currently defined, so this parameter should be zero.

5.4.2 BCryptImportKeyPair

```
NTSTATUS WINAPI BCryptImportKeyPair(
        BCRYPT_ALG_HANDLE hAlgorithm,
        BCRYPT_KEY_HANDLE hImportKey,
        LPCWSTR pszBlobType,
        BCRYPT_KEY_HANDLE *phKey,
        PUCHAR   pbInput,
        ULONG   cbInput,
        ULONG   dwFlags);
```

The BCryptImportKeyPair() function is used to import a public/private key pair from a key blob.
hAlgorithm [in] is the handle of the algorithm provider to import the key. This handle is obtained by calling the BCryptOpenAlgorithmProvider function.
hImportKey [in, out] is not currently used and should be NULL.
pszBlobType [in] is a null-terminated Unicode string that contains an identifier that specifies the type of BLOB that is contained in the pbInput buffer. This can be one of the following values: BCRYPT_DH_PRIVATE_BLOB, BCRYPT_DH_PUBLIC_BLOB, BCRYPT_DSA_PRIVATE_BLOB, BCRYPT_DSA_PUBLIC_BLOB, BCRYPT_PUBLIC_KEY_BLOB, BCRYPT_PRIVATE_KEY_BLOB, BCRYPT_RSAPRIVATE_BLOB, BCRYPT_RSAPUBLIC_BLOB, LEGACY_DH_PUBLIC_BLOB, LEGACY_DH_PRIVATE_BLOB, LEGACY_DSA_PRIVATE_BLOB, LEGACY_DSA_PUBLIC_BLOB, LEGACY_DSA_V2_PRIVATE_BLOB, LEGACY_RSAPRIVATE_BLOB, LEGACY_RSAPUBLIC_BLOB.
phKey [out] is a pointer to a BCRYPT_KEY_HANDLE that receives the handle of the imported key. This handle is used in subsequent functions that require a key, such as BCryptSignHash. This handle must be released when it is no longer needed by passing it to the BCryptDestroyKey function.
pbInput [in] is the address of a buffer that contains the key BLOB to import. The cbInput parameter contains the size of this buffer. The pszBlobType parameter specifies the type of key BLOB this buffer contains.
cbInput [in] contains the size, in bytes, of the pbInput buffer.
dwFlags [in] is a set of flags that modify the behavior of this function. This can be zero or the following value: BCRYPT_NO_KEY_VALIDATION.

5.4.3 BCryptExportKey

```
NTSTATUS WINAPI BCryptExportKey(
        BCRYPT_KEY_HANDLE   hKey,
        BCRYPT_KEY_HANDLE   hExportKey,
        LPCWSTR pszBlobType,
        PUCHAR   pbOutput,
        ULONG   cbOutput,
        ULONG   *pcbResult,
        ULONG   dwFlags);
```

The BCryptExportKey() function exports a key to a memory blob that can be persisted for later use.
hKey [in] is the handle of the key to export.
hExportKey [in, out] is not currently used and should be set to NULL.
pszBlobType [in] is a null-terminated Unicode string that contains an identifier that specifies the type of BLOB to export. This can be one of the following values: BCRYPT_DH_PRIVATE_BLOB, BCRYPT_DH_PUBLIC_BLOB, BCRYPT_DSA_PRIVATE_BLOB, BCRYPT_DSA_PUBLIC_BLOB, BCRYPT_ECCPRIVATE_BLOB, BCRYPT_ECCPUBLIC_BLOB, BCRYPT_KEY_DATA_BLOB, BCRYPT_OPAQUE_KEY_BLOB, BCRYPT_PUBLIC_KEY_BLOB, BCRYPT_PRIVATE_KEY_BLOB, BCRYPT_RSAPRIVATE_BLOB, BCRYPT_RSAPUBLIC_BLOB, LEGACY_DH_PRIVATE_BLOB, LEGACY_DH_PUBLIC_BLOB, LEGACY_DSA_PRIVATE_BLOB, LEGACY_DSA_PUBLIC_BLOB, LEGACY_DSA_V2_PRIVATE_BLOB, LEGACY_RSAPRIVATE_BLOB, LEGACY_RSAPUBLIC_BLOB.

pbOutput is the address of a buffer that receives the key BLOB. The cbOutput parameter contains the size of this buffer. If this parameter is NULL, this function will place the required size, in bytes, in the ULONG pointed to by the pcbResult parameter.
cbOutput [in] contains the size, in bytes, of the pbOutput buffer.
pcbResult [out] is a pointer to a ULONG that receives the number of bytes that were copied to the pbOutput buffer. If the pbOutput parameter is NULL, this function will place the required size, in bytes, in the ULONG pointed to by this parameter.
dwFlags [in] is a set of flags that modify the behavior of this function. No flags are defined for this function.

5.5 Encryption and Decryption

5.5.1 BCryptEncrypt

```
NTSTATUS WINAPI BCryptEncrypt(
        BCRYPT_KEY_HANDLE hKey,
        PUCHAR   pbInput,
        ULONG   cbInput,
        VOID    *pPaddingInfo,
        PUCHAR   pbIV,
        ULONG   cbIV,
        PUCHAR   pbOutput,
        ULONG   cbOutput,
        ULONG   *pcbResult,
        ULONG   dwFlags);
```

The BCryptEncrypt() function encrypts a block of data of given length.
hKey [in, out] is the handle of the key to use to encrypt the data. This handle is obtained from one of the key creation functions, such as BCryptGenerateSymmetricKey, BCryptGenerateKeyPair, or BCryptImportKey.
pbInput [in] is the address of a buffer that contains the plaintext to be encrypted. The cbInput parameter contains the size of the plaintext to encrypt. For more information, see Remarks.
cbInput [in] is the number of bytes in the pbInput buffer to encrypt.
pPaddingInfo [in, optional] is a pointer to a structure that contains padding information. The actual type of structure this parameter points to depends on the value of the dwFlags parameter. This parameter is only used with asymmetric keys and must be NULL otherwise.
pbIV [in, out, optional] is the address of a buffer that contains the initialization vector (IV) to use during encryption. The cbIV parameter contains the size of this buffer. This function will modify the contents of this buffer. If you need to reuse the IV later, make sure you make a copy of this buffer before calling this function. This parameter is optional and can be NULL if no IV is used. The required size of the IV can be obtained by calling the BCryptGetProperty function to get the BCRYPT_BLOCK_LENGTH property. This will provide the size of a block for the algorithm, which is also the size of the IV.
cbIV [in] contains the size, in bytes, of the pbIV buffer.
pbOutput [out, optional] is the address of a buffer that will receive the ciphertext produced by this function. The cbOutput parameter contains the size of this buffer. For more information, see Remarks. If this parameter is NULL, this function will calculate the size needed for the ciphertext and return the size in the location pointed to by the pcbResult parameter.
cbOutput [in] contains the size, in bytes, of the pbOutput buffer. This parameter is ignored if the pbOutput parameter is NULL.
pcbResult [out] is a pointer to a ULONG variable that receives the number of bytes copied to the pbOutput buffer. If pbOutput is NULL, this receives the size, in bytes, required for the ciphertext.
dwFlags [in] is a set of flags that modify the behavior of this function. The allowed set of flags depends on the type of key specified by the hKey parameter. If the key is a symmetric key, this can be zero or the following value: BCRYPT_BLOCK_PADDING. If the key is an asymmetric key, this can be one of the following values: BCRYPT_PAD_NONE, BCRYPT_PAD_OAEP, BCRYPT_PAD_PKCS1.

5.5.2 BCryptDecrypt

```
NTSTATUS WINAPI BCryptDecrypt(
        BCRYPT_KEY_HANDLE   hKey,
        PUCHAR   pbInput,
        ULONG   cbInput,
        VOID    *pPaddingInfo,
        PUCHAR   pbIV,
        ULONG   cbIV,
        PUCHAR   pbOutput,
        ULONG   cbOutput,
        ULONG   *pcbResult,
        ULONG   dwFlags);
```

The BCryptDecrypt() function decrypts a block of data of given length.
hKey [in, out] is the handle of the key to use to decrypt the data. This handle is obtained from one of the key creation functions, such as BCryptGenerateSymmetricKey, BCryptGenerateKeyPair, or BCryptImportKey.
pbInput [in] is the address of a buffer that contains the ciphertext to be decrypted. The cbInput parameter contains the size of the ciphertext to decrypt. For more information, see Remarks.
cbInput [in] is the number of bytes in the pbInput buffer to decrypt.
pPaddingInfo [in, optional] is a pointer to a structure that contains padding information. The actual type of structure this parameter points to depends on the value of the dwFlags parameter. This parameter is only used with asymmetric keys and must be NULL otherwise.
pbIV [in, out, optional] is the address of a buffer that contains the initialization vector (IV) to use during decryption. The cbIV parameter contains the size of this buffer. This function will modify the contents of this buffer. If you need to reuse the IV later, make sure you make a copy of this buffer before calling this function. This parameter is optional and can be NULL if no IV is used. The required size of the IV can be obtained by calling the BCryptGetProperty function to get the BCRYPT_BLOCK_LENGTH property. This will provide the size of a block for the algorithm, which is also the size of the IV.
cbIV [in] contains the size, in bytes, of the pbIV buffer.
pbOutput [out, optional] is the address of a buffer to receive the plaintext produced by this function. The cbOutput parameter contains the size of this buffer. For more information, see Remarks.
If this parameter is NULL, this function will calculate the size required for the plaintext and return the size in the location pointed to by the pcbResult parameter.
cbOutput [in] is the size, in bytes, of the pbOutput buffer. This parameter is ignored if the pbOutput parameter is NULL.
pcbResult [out] is a pointer to a ULONG variable to receive the number of bytes copied to the pbOutput buffer. If pbOutput is NULL, this receives the size, in bytes, required for the plaintext.
dwFlags [in] is a set of flags that modify the behavior of this function. The allowed set of flags depends on the type of key specified by the hKey parameter. If the key is a symmetric key, this can be zero or the following value: BCRYPT_BLOCK_PADDING. If the key is an asymmetric key, this can be one of the following values: BCRYPT_PAD_NONE, BCRYPT_PAD_OAEP, BCRYPT_PAD_PKCS1.

5.6 Hashing and HMAC

5.6.1 BCryptCreateHash

```
NTSTATUS WINAPI BCryptCreateHash(
        BCRYPT_ALG_HANDLE   hAlgorithm,
        BCRYPT_HASH_HANDLE  *phHash,
        PUCHAR   pbHashObject,
        ULONG   cbHashObject,
        PUCHAR   pbSecret,
        ULONG   cbSecret,
        ULONG   dwFlags);
```

The BCryptCreateHash() function creates a hash object with an optional key. The optional key is used for HMAC type keyed-hash functions.
hAlgorithm [in, out] is the handle of an algorithm provider created by using the BCryptOpenAlgorithmProvider function. The algorithm that was specified when the provider was created must support the hash interface.
phHash [out] is a pointer to a BCRYPT_HASH_HANDLE value that receives a handle that represents the hash object. This handle is used in subsequent hashing functions, such as the BCryptHashData function. When you have finished using this handle, release it by passing it to the BCryptDestroyHash function.
pbHashObject [out] is a pointer to a buffer that receives the hash object. The cbHashObject parameter contains the size of this buffer. The required size of this buffer can be obtained by calling the BCryptGetProperty function to get the BCRYPT_OBJECT_LENGTH property. This will provide the size of the hash object for the specified algorithm. This memory can only be freed after the hash handle is destroyed.
cbHashObject [in] contains the size, in bytes, of the pbHashObject buffer.
pbSecret [in, optional] is a pointer to a buffer that contains the key to use for the hash. The cbSecret parameter contains the size of this buffer. If no key should be used with the hash, set this parameter to NULL. This key only applies to keyed hash algorithms, like Hash-Based Message Authentication Code (HMAC).
cbSecret [in, optional] contains the size, in bytes, of the pbSecret buffer. If no key should be used with the hash, set this parameter to zero.
dwFlags [in] is not currently used and must be zero.

5.6.2 BCryptHashData

```
NTSTATUS WINAPI BCryptHashData(
        BCRYPT_HASH_HANDLE  hHash,
        PUCHAR   pbInput,
        ULONG   cbInput,
        ULONG   dwFlags);
```

The BCryptHashData() function performs a one way hash on a data buffer. Call the BCryptFinishHash() function to finalize the hashing operation to get the hash result.

5.6.3 BCryptDuplicateHash

```
NTSTATUS WINAPI BCryptDuplicateHash(
        BCRYPT_HASH_HANDLE  hHash,
        BCRYPT_HASH_HANDLE  *phNewHash,
        PUCHAR   pbHashObject,
        ULONG   cbHashObject,
        ULONG   dwFlags);
```

The BCryptDuplicateHash()function duplicates an existing hash object. The duplicate hash object contains all state and data that was hashed to the point of duplication.

5.6.4 BCryptFinishHash

```
NTSTATUS WINAPI BCryptFinishHash(
        BCRYPT_HASH_HANDLE hHash,
        PUCHAR   pbOutput,
        ULONG   cbOutput,
        ULONG   dwFlags);
```

The BCryptFinishHash() function retrieves the hash value for the data accumulated from prior calls to BCryptHashData() function.

5.6.5 BCryptDestroyHash

```
NTSTATUS WINAPI BCryptDestroyHash(
```

BCRYPT_HASH_HANDLE hHash);

The BCryptDestroyHash() function destroys a hash object.

5.7 Signing and Verification

5.7.1 BCryptSignHash

```
NTSTATUS WINAPI BCryptSignHash(
        BCRYPT_KEY_HANDLE   hKey,
        VOID    *pPaddingInfo,
        PUCHAR   pbInput,
        ULONG   cbInput,
        PUCHAR   pbOutput,
        ULONG   cbOutput,
        ULONG   *pcbResult,
        ULONG   dwFlags);
```

The BCryptSignHash() function creates a signature of a hash value.

hKey [in] is the handle of the key to use to sign the hash.

pPaddingInfo [in, optional] is a pointer to a structure that contains padding information. The actual type of structure this parameter points to depends on the value of the dwFlags parameter. This parameter is only used with asymmetric keys and must be NULL otherwise.

pbInput [in] is a pointer to a buffer that contains the hash value to sign. The cbInput parameter contains the size of this buffer.

cbInput [in] is the number of bytes in the pbInput buffer to sign.

pbOutput [out] is the address of a buffer to receive the signature produced by this function. The cbOutput parameter contains the size of this buffer. If this parameter is NULL, this function will calculate the size required for the signature and return the size in the location pointed to by the pcbResult parameter.

cbOutput [in] is the size, in bytes, of the pbOutput buffer. This parameter is ignored if the pbOutput parameter is NULL.

pcbResult [out] is a pointer to a ULONG variable that receives the number of bytes copied to the pbOutput buffer. If pbOutput is NULL, this receives the size, in bytes, required for the signature.

dwFlags [in] is a set of flags that modify the behavior of this function. The allowed set of flags depends on the type of key specified by the hKey parameter. If the key is a symmetric key, this parameter is not used and should be set to zero. If the key is an asymmetric key, this can be one of the following values: BCRYPT_PAD_PKCS1, BCRYPT_PAD_PSS.

5.7.2 BCryptVerifySignature

```
NTSTATUS WINAPI BCryptVerifySignature(
        BCRYPT_KEY_HANDLE   hKey,
        VOID    *pPaddingInfo,
        PUCHAR   pbHash,
        ULONG   cbHash,
        PUCHAR   pbSignature,
        ULONG   cbSignature,
        ULONG   dwFlags);
```

The BCryptVerifySignature() function verifies that the specified signature matches the specified hash.

hKey [in] is the handle of the key to use to decrypt the signature. This must be an identical key or the public key portion of the key pair used to sign the data with the BCryptSignHash function.

pPaddingInfo [in, optional] is a pointer to a structure that contains padding information. The actual type of structure this parameter points to depends on the value of the *dwFlags* parameter. This parameter is only used with asymmetric keys and must be NULL otherwise.

pbHash [in] is the address of a buffer that contains the hash of the data. The cbHash parameter contains the size of this buffer.

cbHash [in] is the size, in bytes, of the pbHash buffer.

pbSignature [in] is the address of a buffer that contains the signed hash of the data. The BCryptSignHash function is used to create the signature. The *cbSignature* parameter contains the size of this buffer.
cbSignature [in] is the size, in bytes, of the pbSignature buffer. The BCryptSignHash function is used to create the signature.

5.8 Secret Agreement and Key Derivation

5.8.1 BCryptSecretAgreement

```
NTSTATUS WINAPI BCryptSecretAgreement(
        BCRYPT_KEY_HANDLE       hPrivKey,
        BCRYPT_KEY_HANDLE       hPubKey,
        BCRYPT_SECRET_HANDLE    *phAgreedSecret,
        ULONG                   dwFlags);
```

The BCryptSecretAgreement() function creates a secret agreement value from a private and a public key. This function is used with Diffie-Hellman (DH) and Elliptic Curve Diffie-Hellman (ECDH) algorithms.
hPrivKey [in] The handle of the private key to use to create the secret agreement value.
hPubKey [in] The handle of the public key to use to create the secret agreement value.
phSecret [out] A pointer to a BCRYPT_SECRET_HANDLE that receives a handle that represents the secret agreement value. This handle must be released by passing it to the BCryptDestroySecret function when it is no longer needed.
dwFlags [in] A set of flags that modify the behavior of this function. This can be zero or the following value: KDF_USE_SECRET_AS_HMAC_KEY_FLAG.

5.8.2 BCryptDeriveKey

```
NTSTATUS WINAPI BCryptDeriveKey(
        BCRYPT_SECRET_HANDLE hSharedSecret,
        LPCWSTR              pwszKDF,
        BCryptBufferDesc     *pParameterList,
        PUCHAR pbDerivedKey,
        ULONG                cbDerivedKey,
        ULONG                *pcbResult,
        ULONG                dwFlags);
```

The BCryptDeriveKey() function derives a key from a secret agreement value.
hSharedSecret [in, optional] is the secret agreement handle to create the key from. This handle is obtained from the BCryptSecretAgreement function.
pwszKDF [in] is a pointer to a null-terminated Unicode string that contains an object identifier (OID) that identifies the key derivation function (KDF) to use to derive the key. This can be one of the following strings: BCRYPT_KDF_HASH (parameters in pParameterList: KDF_HASH_ALGORITHM, KDF_SECRET_PREPEND, KDF_SECRET_APPEND), BCRYPT_KDF_HMAC (parameters in pParameterList: KDF_HASH_ALGORITHM, KDF_HMAC_KEY, KDF_SECRET_PREPEND, KDF_SECRET_APPEND), BCRYPT_KDF_TLS_PRF (parameters in pParameterList: KDF_TLS_PRF_LABEL, KDF_TLS_PRF_SEED).
pParameterList [in, optional] is the address of a BCryptBufferDesc structure that contains the KDF parameters. This parameter is optional and can be NULL if it is not needed.
pbDerivedKey [out, optional] is the address of a buffer that receives the key. The cbDerivedKey parameter contains the size of this buffer. If this parameter is NULL, this function will place the required size, in bytes, in the ULONG pointed to by the pcbResult parameter.
cbDerivedKey [in] contains the size, in bytes, of the pbDerivedKey buffer.
pcbResult [out] is a pointer to a ULONG that receives the number of bytes that were copied to the pbDerivedKey buffer. If the pbDerivedKey parameter is NULL, this function will place the required size, in bytes, in the ULONG pointed to by this parameter.
dwFlags [in] is a set of flags that modify the behavior of this function. This can be zero or the following value.

5.8.3 BCryptDestroySecret

NTSTATUS WINAPI BCryptDestroySecret(
BCRYPT_SECRET_HANDLE hSecret);

The BCryptDestroySecret() function destroys a secret agreement handle that was created by using the BCryptSecretAgreement() function.

5.9 Configuration

These are not cryptographic functions. They are used to configure cryptographic providers on the system, and are provided for informational purposes. Please see http://msdn.microsoft.com for details.

Function Name	Description
BCryptAddContextFunction	Adds a function (algorithm or cipher-suite) to a context function list.
BCryptAddContextFunctionProvider	Adds a provider to a context function provider list.
BCryptConfigureContext	Configures a context.
BCryptConfigureContextFunction	Configures a context function.
BCryptConfigureContextFunction	Configures a context function.
BCryptCreateContext	Creates a new configuration context.
BCryptDeleteContext	Deletes a configuration context.
BCryptEnumAlgorithms	Enumerates the algorithms for a given set of operations.
BCryptEnumContextFunctionProviders	Enumerates the providers in a context function provider list.
BCryptEnumContextFunctions	Enumerates the functions (algorithms or suites) in a context function list.
BCryptEnumContexts	Enumerates the configuration contexts in the specified table.
BCryptEnumProviders	Returns a list of providers for a given algorithm.
BCryptEnumRegisteredProviders	Enumerates the providers currently registered on the local machine.
BCryptQueryContextConfiguration	Queries the current configuration of a context.
BCryptQueryContextFunctionConfiguration	Queries the current configuration of a context function.
BCryptQueryContextFunctionProperty	Queries the current value of a context function property.
BCryptQueryProviderRegistration	Retrieves registration information for a provider.
BCryptRegisterConfigChangeNotify	This API differs slightly between User-Mode and Kernel-Mode.
BCryptRegisterProvider	Registers a provider for usage on the local machine.
BCryptRemoveContextFunction	Removes a function (algorithm or cipher-suite) from a context function list.
BCryptRemoveContextFunctionProvider	Removes a provider from a context function provider list.
BCryptResolveProviders	This is the main API in Crypto configuration. It resolves queries against the set of providers currently registered on the local system and the configuration information specified in the machine and domain configuration tables, returning an ordered list of references to one or more providers matching the specified criteria.
BCryptSetContextFunctionProperty	Creates, modifies, or deletes a context function property.
BCryptUnregisterConfigChangeNotify	This API differs slightly between User-Mode and Kernel-Mode.
BCryptUnregisterProvider	Removes provider registration information from the local machine.

6 Operational Environment

BCRYPT.DLL is intended to run on Windows Vista in Single User mode as defined in Section 2. When run in this configuration, multiple concurrent operators are not supported.
Because BCRYPT.DLL module is a DLL, each process requesting access is provided its own instance of the module. As such, each process has full access to all information and keys within the module. Note that no keys or other information are maintained upon detachment from the DLL, thus an instantiation of the module will only contain keys or information that the process has placed in the module.

7 Cryptographic Key Management

BCRYPT.DLL crypto module manages keys in the following manner.

7.1 Cryptographic Keys, CSPs, and SRDIs

The BCRYPT.DLL crypto module contains the following security relevant data items:

Security Relevant Data Item	SRDI Description
Symmetric encryption/decryption keys	Keys used for AES or TDES encryption/decryption.
HMAC keys	Keys used for HMAC-SHA1, HMAC-SHA256, HMAC-SHA384, and HMAC-SHA512
DSA Public Keys	Keys used for the verification of DSA digital signatures
DSA Private Keys	Keys used for the calculation of DSA digital signatures
ECDSA Public Keys	Keys used for the verification of ECDSA digital signatures
ECDSA Private Keys	Keys used for the calculation of ECDSA digital signatures
RSA Public Keys	Keys used for the verification of RSA digital signatures
RSA Private Keys	Keys used for the calculation of RSA digital signatures
DH Public and Private values	Public and private values used for Diffie-Hellman key establishment.
ECDH Public and Private values	Public and private values used for EC Diffie-Hellman key establishment.

7.2 Access Control Policy

The BCRYPT.DLL crypto module allows controlled access to the SRDIs contained within it. The following table defines the access that a service has to each. The permissions are categorized as a set of four separate permissions: read (r), write (w), execute (x), delete (d). If no permission is listed, the service has no access to the SRDI.

BCRYPT.DLL crypto module SRDI/Service Access Policy	Security Relevant Data Item	Symmetric encryption/decryption keys	HMAC keys	DSA Public Keys	DSA Private Keys	ECDSA public keys	ECDSA Private keys	RSA Public Keys	RSA Private Keys	DH Public and Private values	ECDH Public and Private values
Service											
Cryptographic Module Power Up and Power Down											
Key Formatting		w									
Random Number Generation											
Data Encryption and Decryption		x									
Hashing			x / w								
Acquiring a Table of Pointers to BCryptXXX Functions											
Algorithm Providers and Properties											
Key and Key-Pair Generation		w / d	w / d	w / d	w / d	w / d	w / d	w / d	w / d	w / d	w / d
Key Entry and Output		r / w	r / w	r / w	r / w	r / w	r / w	r / w	r / w	r / w	r / w
Signing and Verification				x	x	x	x	x	x		
Secret Agreement and Key Derivation										x	x

7.3 Key Material

Each time an application links with BCRYPT.DLL, the DLL is instantiated and no keys exist within it. The user application is responsible for importing keys into BCRYPT.DLL or using BCRYPT.DLL's functions to generate keys.

7.4 Key Generation

BCRYPT.DLL can create and use keys for the following algorithms: RSA, DSA, DH, ECDH, ECDSA, RC2, RC4, DES, Triple-DES, AES, and HMAC.
Random keys can be generated by calling the BCryptGenerateSymmetricKey() and BCryptGenerateKeyPair() functions. Random data generated by the BCryptGenRandom() function is provided to BCryptGenerateSymmetricKey() function to generate symmetric keys. DES, Triple-DES, AES, RSA, ECDSA, DSA, DH, and ECDH keys and key-pairs are generated following the techniques given in section 5.2.

7.5 Key Establishment

BCRYPT.DLL can use FIPS approved Diffie-Hellman key agreement (DH), Elliptic Curve Diffie-Hellman key agreement (ECDH), and manual methods to establish keys.
BCRYPT.DLL can use the following FIPS approved key derivation functions (KDF) from the common secret that is established during the execution of DH and ECDH key agreement algorithms:

- BCRYPT_KDF_HASH. This KDF supports FIPS approved SP800-56A (Section 5.8), X9.63, and X9.42 key derivation.
- BCRYPT_KDF_HMAC. This KDF supports FIPS approved IPsec IKE v1 key derivation as specified in FIPS 140-2 Implementation Guidance.
- BCRYPT_KDF_TLS_PRF. This KDF supports FIPS approved SSLv3.1 and TLS v1.0 key derivation as specified in FIPS 140-2 Implementation Guidance.

7.6 Key Entry and Output

Keys can be both exported and imported out of and into BCRYPT.DLL via BCryptExportKey(), BCryptImportKey(), and BCryptImportKeyPair() functions.
Symmetric key entry and output can also be done by exchanging keys using the recipient's asymmetric public key via BCryptSecretAgreement() and BCryptDeriveKey() functions.

Exporting the RSA private key by supplying a blob type of BCRYPT_PRIVATE_KEY_BLOB, BCRYPT_RSAFULLPRIVATE_BLOB, or BCRYPT_RSAPRIVATE_BLOB to BCryptExportKey() is not allowed in FIPS mode.

7.7 Key Storage

BCRYPT.DLL does not provide persistent storage of keys.

7.8 Key Archival

BCRYPT.DLL does not directly archive cryptographic keys. The Authenticated User may choose to export a cryptographic key (cf. "Key Entry and Output" above), but management of the secure archival of that key is the responsibility of the user.

7.9 Key Zeroization

All keys are destroyed and their memory location zeroized when the Authenticated User calls BCryptDestroyKey() or BCryptDestroySecret() on that key handle.

8 Self-Tests

BCRYPT.DLL performs the following power-on (start up) self-tests when DllMain is called by the operating system.

- SHA-1 hash Known Answer Test
- HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 Known Answer Test
- Triple-DES encrypt/decrypt EBC Known Answer Test
- Triple-DES encrypt/decrypt CBC Known Answer Test
- AES-128, AES-192, AES-256 encrypt/decrypt EBC Known Answer Test
- AES-128, AES-192, AES-256 encrypt/decrypt CBC Known Answer Test
- AES-128, AES-192, AES-256 encrypt/decrypt CFB with 8-bit feedback Known Answer Test
- AES-128, AES-192, AES-256 GMAC Known Answer Test
- AES-128, AES-192, AES-256 encrypt/decrypt CCM Known Answer Test
- AES-128, AES-192, AES-256 encrypt/decrypt GCM Known Answer Test
- DSA sign/verify test
- RSA sign and verify test
- DH secret agreement Known Answer Test
- ECDSA sign/verify test

- ECDH secret agreement Known Answer Test
- FIPS 186-2 DSA random generator Known Answer Tests
- SP800-90 AES-256 based counter mode random generator Known Answer Test

BCRYPT.DLL performs pair-wise consistency checks upon each invocation of RSA, ECDH, DSA, and ECDSA key-pair generation and import as defined in FIPS 140-2. BCRYPT.DLL also performs a continuous RNG test on each of the implemented RNGs as defined in FIPS 140-2.

In all cases for any failure of a power-on (start up) self-test, BCRYPT.DLL DllMain fails to return the STATUS_SUCCESS status to the operating system. The only way to recover from the failure of a power-on (start up) self-test is to attempt to reload the BCRYPT.DLL, which will rerun the self-tests, and will only succeed if the self-tests passes.

9 Design Assurance

The BCRYPT.DLL crypto module is part of the overall Windows Vista operating system, which is a product family that has gone through and is continuously going through the Common Criteria Certification or equivalent under US NIAP CCEVS since Windows NT 3.5. The certification provides the necessary design assurance.
The BCRYPT.DLL is installed and started as part of the Windows Vista operating system.

10 Additional details

For the latest information on Windows Vista, check out the Microsoft web site at http://www.microsoft.com.

CHANGE HISTORY			
AUTHOR	**DATE**	**VERSION**	**COMMENT**
Tolga Acar	6/7/2007	1.0	FIPS Approval Submission
Stefan Santesson	2/15/2008	1.2	Merged changes resulting from Gold CMVP review
Stefan Santesson	10/30/2007	1.1	Added technical updates related to SP1 and WS2K8