BitLocker Drive Encryption (BDE) format specification

Analysis of theBitLocker Drive Encryption (BDE) volume format

By Joachim Metz <joachim.metz@gmail.com>

Summary

The BitLocker Drive Encryption (BDE) format is used by Microsoft Windows to encrypt volumes. This specification is based on available documentation and was enhanced by reverse engineering of the file format.

This document is intended as a working document for the BitLocker Drive Encryption (BDE) format specification. Which should allow existing Open Source forensic tooling to be able to process this volume type.

Document information

Author(s): Joachim Metz <joachim.metz@gmail.com>

Abstract: This document contains information about the BitLocker Drive Encryption (BDE) format

Classification: Public

Keywords: BitLocker Drive Encryption, BDE, Full Volume Encryption, FVE

License

Version

Version	Author	Date	Comments
0.0.1	J.B. Metz	March 2011 May 2011 June 2011 July 2011 August 2011 September 2011	Worked on initial version.
0.0.2	J.B. Metz	October 2011	Additional information.
0.0.3	J.B. Metz	May 2012	Updates for Windows 8 Consumer Preview.
0.0.4	J.B. Metz	June 2013	Additional information regarding Windows 8 with thanks to T. Duc Nguyen.
0.0.5	J.B. Metz	June 2013	Additional information regarding encryption method MSB with thanks to S. Hansen.
0.0.6	J.B. Metz	June 2014	Additional information regarding encryption method MSB with thanks to J. Van Tubbergh.

Table of Contents

1. Overview

BitLocker Drive Encrypting (BDE) is the volume encryption used by Microsoft Windows as of Vista. There are multiple versions of BitLocker Drive Encryption (BDE):

- BitLocker Windows Vista
- TODO: BitLocker Windows 2008
- BitLocker Windows 7
- BitLocker To Go
- BitLocker Windows 8

Both BitLocker Windows Vista and BitLocker Windows 7 are intended to encrypt NTFS volumes on fixed storage media, like harddisks. BitLocker To Go was introduced in Windows 7 and is intended to encrypt removable drives, with e.g. FAT file systems. NTFS volumes on removable drives are treated as NTFS volumes on fixed storage media.

The BitLocker identifier (GUID) is 4967d63b-2e29-4ad8-8399-f6a339e3d00.

BitLocker To Go uses 4967d63b-2e29-4ad8-8399-f6a339e3d01.

1.1. Metadata files

1.1.1. Windows Vista

In Windows Vista the System Volume Information folder of the unencrypted volume contain several file entries for the BitLocker metadata blocks:

- FVE.{%GUID%}.[123] maps the blocks that contain the FVE metadata. Typically 16384 bytes of size.

The contents of the metadata files, on an unencrypted volume, consists of 0-byte values. It is assumed that these files are used to prevent the BitLocker metadata to be overwritten.

Note that EnCase (at least version 6.18) does not zero out these metadata areas.

1.1.2. Windows 7

In Windows 7 the System Volume Information folder of the unencrypted volume contain several file entries for the BitLocker metadata blocks:

- FVE2.{%GUID%} maps the block that contains the encrypted volume header. Typically 8192 bytes of size.
- FVE2.{%GUID%}.[123] maps the blocks that contain the FVE metadata. Typically 65536 bytes of size.

The contents of the metadata files, on an unencrypted volume, consists of 0-byte values. It is assumed that these files are used to prevent the BitLocker metadata to be overwritten.

Note that EnCase (at least version 6.18) does not zero out these metadata areas.

1.1.3. To Go

BitLocker To Go uses a hybrid volume that has a encrypted and an unencrypted part. The unencrypted part contains various files.

- Application files for the BitLocker To Go helper application; which can also be found in C:\Windows\BitLockerDiscoveryVolumeContents\
- “COV 0000. BL” maps the block that contains the BitLocker To Go GUID and the offsets to the metadata. Typically 32768 bytes of size.
- “COV 0000. ER” maps the encrypted data.
- “PAD 0000. PD” maps padding.
- “PAD 0000. NG” unknown. Typically 0 bytes of size.

2. Keys

To encrypt storage media BitLocker uses different kind of keys.

2.1. Volume Master Key (VMK)

The Volume Master Key (VMK) is 256-bit of size and is stored in multiple FVE Volume Master Key (VMK) structures. The VMK is stored encrypted with either the recovery key, external key, or the TPM.

It is also possible that the VMK is stored unencrypted which is referred to as clear key.

2.2. Full Volume Encryption Key (FVEK)

The Full Volume Encryption Key (FVEK) is stored encrypted with the Volume Master Key (VMK). The size of the FVEK is dependent on the encryption method used:

- For AES 128-bit the key is 128-bit of size
- For AES 256-bit the key is 256-bit of size

When Elephant Diffuser is used the key data of the structure that hold the FKEV is always 512-bit of size. The First 256-bit are reserved for the FVEK and the other 256-bit for the TWEAK key. Only 128-bit of the 256-bits are used when the encryption method is AES 128-bit.

2.3. TWEAK key

The TWEAK is stored encrypted with the Volume Master Key (VMK). The size of the TWEAK key is dependent on the encryption method used:

- For AES 128-bit the key is 128-bit of size
- For AES 256-bit the key is 256-bit of size

The TWEAK key is only present when Elephant Diffuser is used. The TWEAK key is stored in the key data of the structure that hold the Full Volume Encryption Key (FVEK) is always 512-bit of size. The First 256-bit are reserved for the FVEK and the other 256-bit for the TWEAK key. Only 128-bit of the 256-bits are used when the encryption method is AES 128-bit.

2.4. Recovery key

BitLocker provides for a recovery (or numerical) password to unlock the encrypted data. The recovery password is used to determine a recovery key.

Example recovery password:
471207-278498-422125-177177-561902-537405-468006-693451

A valid recovery password consists of 48 digits where every number is dividable by 11 with a remainder of 0. The result of a division by 11 of a number is a 16-bit value. The individual 16-bit values make up a 128-bit key.

The corresponding recovery key is calculated using the following approach, written partially in pseudo C:

Initialize a structure consisting of:

```
uint8_t last_sha256[ 32 ];
uint8_t initial_sha256[ 32 ];
uint8_t salt[ 16 ];
uint64_t count;
```

Initialize both the last SHA256 and the count to 0.
Calculate the SHA256 of the 128-bit key and update the initial SHA256 value.

The salt is stored on disk in the stretch key which is stored in the recovery key protected Volume Master Key (VMK).

Loop for 1048576 (0x100000) times:

- calculate the SHA256 of the structure and update the last SHA256 value
- increment the count by 1

The last SHA256 value contains the 256-bit key which is recovery key that can unlock the recovery key protected Volume Master Key (VMK).

2.5. Clear key

The clear key is an unprotected 256-bit key stored on the volume to decrypt the VMK. It is used when the encrypted volume is being decrypted.

2.6. Startup key

The startup key (or external key) is stored in a file named {%GUID%}.BEK. The GUID in the filename equals the key identifier in the BitLocker metadata.

There can be multiple startup keys for a single BitLocker volume. Each key is identified a by a different key identifier.

2.7. User key

BitLocker To Go provides for a user password (or passphrase) to unlock the encrypted data. The user password is used to determine a user key.

TODO check this:
The password can be maximal 49 characters in size.

Convert the user password into a UTF16 little-endian string.

Initialize a structure consisting of:

```
uint8_t last_sha256[ 32 ];
uint8_t initial_sha256[ 32 ];
uint8_t salt[ 16 ];
uint64_t count;
```

Initialize both the last SHA256 and the count to 0.
Calculate the SHA256 of the user password.
Calculate the SHA256 of the SHA256 of the user password, and set it as the initial SHA256 value.

The salt is stored on disk in the stretch key which is stored in the user key (or password) protected Volume Master Key (VMK).

Loop for 1048576 (0x100000) times:

- calculate the SHA256 of the structure and update the last SHA256 value
- increment the count by 1

The last SHA256 value contains the 256-bit key which is user key that can unlock the user key (or password) protected Volume Master Key (VMK).

3. Encryption methods

BitLocker uses different kind of encryption methods. To encrypt the sector data it either uses AES-CBC with or without Elephant Elephant Diffuser. To encrypt the key data BitLocker uses AES-CCM.

3.1. AES-CBC

Both encryption and decryption use:

- AES-CBC with FVEK decryption of sector data

The initialization vector of the AES-CBC is determined by AES-ECB encrypting the sector offset with the FVEK. The sector offset is a 16-byte little-endian version of the offset of the sector relative from the start of the volume.

3.2. AES-CBC with Elephant Diffuser

Encryption:

- XOR with sector key
- Elephant Elephant Diffuser A
- Elephant Elephant Diffuser B
- AES-CBC with FVEK

Decryption

- AES-CBC with FVEK
- Elephant Elephant Diffuser B
- Elephant Elephant Diffuser A
- XOR with sector key

The initialization vector of the AES-CBC is determined by AES-ECB encrypting the sector offset with the FVEK. The sector offset is a 16-byte little-endian version of the offset of the sector relative from the start of the volume.

The sector key 32-byte of size and contains:

- the lower 16-byte contain a little-endian version of the offset of the sector, relative from the start of the volume, AES-ECB encrypted with the TWEAK key
- the upper 16-byte contain a 16-byte little-endian version of the offset of the sector, relative from the start of the volume, with the most upper bit set (or upper byte set to 0x80) AES-ECB encrypted with the TWEAK key

3.3. AES-CCM

The key data is encrypted using AES-CCM with an initialization vector of 0.

3.4. Elephant Diffuser

The Elephant Diffuser A and B variants are described in [FERGUSON06].

3.5. Virtual sector(s)

In BitLocker the certain sector(s) of the encrypted storage media are handled in a specific manner. These are sectors to store:

- the unencrypted volume header

- the BitLocker metadata

3.5.1. BitLocker Windows Vista

In BitLocker Windows Vista the first sector of the unencrypted volume header sector is reconstructed by replacing values in the BitLocker Volume header, namely

- replacing the “File system signature” with “NTFS\x20\x20\x20\x20”
- replacing the “FVE metadata block 1 cluster block number” with the “MTF mirror cluster block number”

The 15 sectors directly following the first sector are also unencrypted.

The sectors that contain the BDE metadata are shown as empty sectors; containing 0-byte values.

Note that EnCase (at least version 6.18) does not zero out these metadata areas.

3.5.2. BitLocker Windows 7 and To Go

Both BitLocker Windows 7 and To Go store an encrypted version of the unencrypted first sectors in a specific location. This location is defined in the FVE Volume header block. It is commonly 8192 bytes an size, entailing the first 16 sectors.

The sectors that contain the encrypted volume header and the BDE metadata are shown as empty sectors; containing 0-byte values.

Note that EnCase (at least version 6.18) does not zero out these metadata areas.

4. Volume header

4.1. BitLocker Windows Vista

The BitLocker Windows Vista volume header is similar to NTFS volume header. The differences have been emphasized in bold. The volume header is 512 bytes of size and consists of:

Offset	Size	Value	Description
0	3	“\xeb\x52\x90”	Boot entry point
3	**8**	**“-FVE-FS-”**	**File system signature**
11	2		Bytes per sector
13	1		Sectors per cluster block
14	2	0x00	Reserved Sectors
16	1	0x00	Number of File Allocation Tables (FATs)
17	2	0	Root directory entries

Offset	Size	Value	Description
19	2		Total number of sectors (16-bit)
21	1		Media descriptor
22	2	0x00	Sectors Per File Allocation Table (FAT)
24	2	0x3f	Sectors per track
26	2		Number of heads
28	4		Number of hidden sectors
32	4	0x00	Total number of sectors (32-bit)
36	1	0x80	Unknown (Disc unit number)
37	1	0x00	Unknown (Flags)
38	1	0x80	Unknown (BPB version signature byte)
39	1	0x00	Unknown (Reserved)
40	8		Total number of sectors (64-bit)
48	8		Master File Table (MFT) cluster block number
56	**8**		**FVE metadata block 1 cluster block number**
64	1		MFT entry size
65	3		Unknown
68	1		Index entry size
69	3		Unknown
72	8		NTFS volume serial number
80	4	0x00	Checksum
84	426		Bootcode
510	2	0x55 0xaa	Sector signature

Note that the number of sectors can be 1 less then the value indicated in the partition table.

4.2. BitLocker Windows 7 and later

The BitLocker Windows 7 (and later) volume header less similar to NTFS volume header than the BitLocker Windows Vista volume header. The differences between the versions have been emphasized in bold. The volume header is 512 bytes of size and consists of:

Offset	Size	Value	Description
0	3	"\xeb**\x58**\x90"	Boot entry point
3	8	"-FVE-FS-"	File system signature
11	2		Bytes per sector
13	1		Sectors per cluster block

Offset	**Size**	**Value**	**Description**
14	2	0x00	Reserved Sectors
16	1	0x00	Number of File Allocation Tables (FATs)
17	2	0	Root directory entries
19	2		Total number of sectors (16-bit)
21	1		Media descriptor
22	2	0x00	Sectors Per File Allocation Table (FAT)
24	2	0x3f	Sectors per track
26	2		Number of heads
28	**4**		**Number of hidden sectors** **Contains the volume start sector number**
32	4	0x00	Total number of sectors (32-bit)
36	**4**	**0x1f0e**	**Sectors per file allocation table**
40	**2**		**FAT Flags (Only used during a conversion from a FAT12/16 volume.)**
42	**2**		**Version (Defined as 0)**
44	**4**		**Cluster number of root directory start**
48	**2**	**0x0001**	**Sector number of FS Information Sector**
50	**2**	**0x0006**	**Sector number of a copy of this boot sector (0 if no backup copy exists)**
52	**12**		**Reserved**
64	**1**	**0x80**	**Physical Drive Number (see FAT12/16 BPB at offset 0x24)**
65	**1**		**Reserved (see FAT12/16 BPB at offset 0x25)**
66	**1**	**0x29**	**Extended boot signature. (see FAT12/16 BPB at offset 0x26)**
67	**4**		**Volume serial number**
71	**11**	**“NO NAME\x20\x20\x20\x20“**	**Volume label**
82	**8**	**"FAT32\x20\x20\x20"**	**File system signature**
90	**70**		**Bootcode**
160	**16**		**BitLocker identifier** **contains a GUID**
176	**8**		**FVE metadata block 1 offset** **Contains an offset relative to the start of the volume**

Offset	Size	Value	Description
184	**8**		**FVE metadata block 2 offset** **Contains an offset relative to the start of the volume**
192	**8**		**FVE metadata block 3 offset** **Contains an offset relative to the start of the volume**
200	**307**		**Unknown (part of bootcode)**
507	**3**		**Unknown**
510	2	0x55 0xaa	Sector signature

Note that the number of sectors can be 1 less then the value indicated in the partition table.

TODO check highlighted values

4.3. BitLocker To Go

BitLocker To Go on an NTFS volume is similar to BitLocker Windows 7. The BitLocker Windows To Go volume header for a FAT volume is similar to FAT32 volume header. The differences have been emphasized in bold. The volume header is 512 bytes of size and consists of:

Offset	Size	Value	Description
0	3	"\xeb\x58\x90"	Boot entry point
3	**8**	**"MSWIN4.1"**	**Signature**
11	2		Bytes per sector
13	1		Sectors per cluster block
14	2	0x00	Reserved Sectors
16	1	0x00	Number of File Allocation Tables (FATs)
17	2	0	Root directory entries
19	2		Total number of sectors (16-bit)
21	1		Media descriptor
22	2	0x00	Sectors Per File Allocation Table (FAT)
24	2	0x3f	Sectors per track
26	2		Number of heads
28	4		Number of hidden sectors
32	4		Total number of sectors (32-bit)
36	4	0x1f0e	Sectors per file allocation table
40	2		FAT Flags (Only used during a conversion from a FAT12/16 volume.)

Offset	Size	Value	Description
42	2		Version (Defined as 0)
44	4		Cluster number of root directory start
48	2	0x0001	Sector number of FS Information Sector
50	2	0x0006	Sector number of a copy of this boot sector (0 if no backup copy exists)
52	12		Reserved
64	1	0x80	Physical Drive Number (see FAT12/16 BPB at offset 0x24)
65	1		Reserved (see FAT12/16 BPB at offset 0x25)
66	1	0x29	Extended boot signature. (see FAT12/16 BPB at offset 0x26)
67	4		Volume serial number
71	11	“NO NAME\x20\x20\x20\x20“	Volume label
82	8	"FAT32\x20\x20\x20"	File system signature
90	334		Bootcode
424	**16**		**BitLocker identifier** **contains a GUID**
440	**8**		**FVE metadata block 1 offset** **Contains an offset relative to the start of the volume**
448	**8**		**FVE metadata block 2 offset** **Contains an offset relative to the start of the volume**
456	**8**		**FVE metadata block 3 offset** **Contains an offset relative to the start of the volume**
464	46		Unknown
510	2	0x55 0xaa	Sector signature

TODO check highlighted values

5. FVE metadata block

A BitLocker volume contains 3 FVE metadata blocks. Each FVE metadata block consists of:

- a block header
- a metadata header

- an array of metadata entries
- padding (0-byte values) (seen in Windows 8)

5.1. FVE metadata block header

5.1.1. FVE metadata block header version 1 - Windows Vista

The FVE metadata block header version 1 is 64 bytes of size and consists of:

Offset	Size	Value	Description
0	8	"-FVE-FS-"	Signature
8	2		Size
10	2	1	Version
12	2		Unknown 0x04 commonly
14	2		Unknown 0x04 commonly
16	16	0	Unknown (empty values)
32	8		FVE metadata block 1 offset Contains an offset relative to the start of the volume
40	8		FVE metadata block 2 offset Contains an offset relative to the start of the volume
48	8		FVE metadata block 3 offset Contains an offset relative to the start of the volume
56	8		MFT mirror cluster block number

5.1.2. FVE metadata block header version 2 – Windows 7 and later

The FVE metadata block header version 2 is 64 bytes of size and consists of:

Offset	Size	Value	Description
0	8	"-FVE-FS-"	Signature
8	2		Size
10	2	2	Version
12	2		Unknown 0x04 commonly 0x05 in partial decrypted volume (protection status?)
14	2		Unknown copy

Offset	Size	Value	Description
			0x04 commonly 0x01 in partial decrypted volume
16	8		Encrypted volume size Contains the number of bytes
24	4		Unknown
28	4		Number of volume header sectors Contains the number of sectors
32	8		FVE metadata block 1 offset Contains an offset relative to the start of the volume
40	8		FVE metadata block 2 offset Contains an offset relative to the start of the volume
48	8		FVE metadata block 3 offset Contains an offset relative to the start of the volume
56	8		**Volume header offset** **Contains an offset relative to the start of the volume**

When decrypting BitLocker will decrypt from the back to the front. The encrypted volume size therefore contains the number of bytes of the volume that are still encrypted (or need to be decrypted).

5.2. FVE metadata header (version 1)

The FVE metadata header (version 1) is 48 bytes of size and consists of:

Offset	Size	Value	Description
0	4		Metadata size Size of the data in the FVE metadata including this size value itself
4	4	1	Version
8	4	48	Metadata header size
12	4		Metadata size copy
16	16		Volume identifier Contains a GUID
32	4		Next nonce counter
36	4		Encryption method See section: 5.2.1 Encryption methods It is currently unknown what the upper 16-bit is used for the MSB has been seen to be used or is

Offset	Size	Value	Description
			this value actually 2x 16-bit values.
40	8		Creation time Contains a filetime

5.2.1. Encryption methods

Value	Identifier	Description
0x0000		Not encrypted/External Key
0x1000		Stretch key
0x1001		Stretch key
0x2000		AES-CCM 256 bit encryption
0x2001		AES-CCM 256 bit encryption
0x2002		AES-CCM 256 bit encryption
0x2003		AES-CCM 256 bit encryption
0x2004		AES-CCM 256 bit encryption
0x2005		AES-CCM 256 bit encryption
0x8000		AES-CBC 128-bit encryption with Elephant Diffuser
0x8001		AES-CBC 256-bit encryption with Elephant Diffuser
0x8002		AES-CBC 128-bit encryption
0x8003		AES-CBC 256-bit encryption

5.3. FVE metadata entry (version 1)

The FVE metadata entry (version 1) is variable of size and consists of:

Offset	Size	Value	Description
0	2		Entry size Size of the data in the FVE metadata entry including this size value itself
2	2		Entry type
4	2		Value type
6	2	1	Version

Offset	Size	Value	Description
8	…		Data

5.3.1. FVE metadata entry types

Value	Identifier	Description
0x0000		None, entry is a property
0x0002		Volume Master Key (VMK)
0x0003		Full Volume Encryption Key (FKEV)
0x0004		Validation
0x0006		Startup key
0x0007		Description (Drive label) Contains computer name, volume name and date Is the date format dependent on the locale MM/DD/YYYY?
0x000b		Unknown: Backup of the Full Volume Encryption Key (FKEV)?
0x000f		Volume header block

5.3.2. FVE metadata value types

Value	Identifier	Description
0x0000		Erased
0x0001		Key
0x0002		Unicode string UTF-16 little-endian with end of string character
0x0003		Stretch Key
0x0004		Use Key
0x0005		AES-CCM encrypted key
0x0006		TPM encoded key
0x0007		Validation
0x0008		Volume master key

Value	Identifier	Description
0x0009		External key
0x000a		Update
0x000b		Error
0x000f		Offset and size tuple of 2 x 64-bit values

5.4. FVE key

The FVE Stretch encrypted key has value type 0x0001. It is variable in size and consists of:

Offset	Size	Value	Description
0	4		Encryption method See section: 5.2.1 Encryption methods
4	…		Key data

5.5. FVE Stretch encrypted key

The FVE Stretch encrypted key has value type 0x0003. It is variable in size and consists of:

Offset	Size	Value	Description
0	4		Encryption method See section: 5.2.1 Encryption methods
4	16		Salt
20	…		FVE metadata entry Contains an AES-CCM encrypted key

5.6. FVE AES-CCM encrypted key

The FVE AES-CCM encrypted key has value type 0x0005. It is variable in size and consists of:

Offset	Size	Value	Description
0	8		Nonce date and time Contains a filetime
8	4		Nonce counter
12	...		AES-CCM encrypted data

5.6.1. Unencrypted data

The unencrypted data is variable of size and consist of:

Offset	Size	Value	Description
0	16		Message Authentication Code (MAC)
Key container			
16	4		Size Does not include the size of the MAC
20	2	1	Version
22	2		Unknown
24	4		Encryption method See section: 5.2.1 Encryption methods
28	...		Unencrypted key data

5.7. FVE TPM encoded key

The FVE TPM encoded key has value type 0x0006. It is variable in size and consists of:

TODO – this structure has not been analyzed yet

5.8. FVE Validation

The FVE Validation has value type 0x0007. It is variable in size and consists of:

TODO – this structure has not been analyzed yet

5.9. FVE Volume Master Key (VMK)

The FVE Volume Master Key has value type 0x0008. It is variable in size and consists of:

Offset	Size	Value	Description
0	16		Key identifier Contains a GUID
16	8		Last modification date and time Contains a filetime
24	2		Unknown
26	2		Protection type See section: 5.9.1 Key protection types
28	...		Properties Contains an array of FVE metadata entries where the entry type is set to 0.

The available properties depend on the VMK type.

The clear key protected VMK consists of:

- key (with 256-bit of key data)
- AES-CCM encrypted key

The recovery key protected VMK consists of:

- optional description string containing “DiskPassword\x00”
- stretch key
- AES-CCM encrypted key

The startup key protected VMK consists of:

- optional description string containing “ExternalKey\x00”
- stretch key
- AES-CCM encrypted key

The password protected VMK consists of:

- optional description string containing “ExternalKey\x00”
- stretch key
- AES-CCM encrypted key

5.9.1. Key protection types

Value	Identifier	Description
0x0000		VMK protected with clear key (Basically this is an unprotected VMK)
0x0100		VMK protected with TPM
0x0200		VMK protected with startup key
0x0800		VMK protected with recovery password
0x2000		VMK protected with password

5.10. FVE External Key

The FVE External Key has value type 0x0009. It is variable in size and consists of:

Offset	Size	Value	Description
0	16		Key identifier Contains a GUID
16	8		Last modification date and time Contains a filetime
24	...		Properties Contains an array of FVE metadata entries where

Offset	Size	Value	Description
			the entry type is set to 0.

The available properties:

- optional description string containing “ExternalKey\x00”
- key

5.11. FVE Volume header block

The FVE Volume header block has value type 0x000f. It is 16 or 52 byte in size and consists of:

Offset	Size	Value	Description
0	8		Block offset
8	8		Block size
Added in Windows 8			
16	8		Unknown
24	8		Unknown
32	12		Unknown (empty values)
44	4		Unknown (sector size?)
48	4		Unknown (sector size?)

The FVE Volume header block seems to have been introduced in Windows 7. It specifies the location in the encrypted volume where the unencrypted volume header is stored.

The FVE Volume header block is commonly 8192 bytes in size for Windows 7 and 5365760 bytes for a BitLocker To Go.

6. BitLocker External Key (BEK) file

A BitLocker External Key (BEK) file is commonly 156 bytes of size and consists of:

- a file header
- an array of metadata entries

6.1. BEK file header (version 1)

The BEK file header is similar to the FVE metadata header (version 1). The BEK file header (version 1) is 48 bytes of size and consists of:

Offset	Size	Value	Description
0	4		Metadata size Size of the remaining data in the file including this size value itself

Offset	Size	Value	Description
4	4	1	Version
8	4	48	Metadata header size
12	4		Metadata size copy
16	16		Volume identifier Contains a GUID
32	4		Next nonce counter
36	4		Encryption method See section: 5.2.1 Encryption methods
40	8		Creation time Contains a filetime

The key identifier in the file must match the key identifier in the FVE Volume Master Key (VMK).

6.2. BEK metadata entry (version 1)

The format of a BEK metadata entry (version 1) is similar to the format of a FVE metadata entry (version 1).

The metadata in a BEK file consists of an FVE external key, which contains 256-bits of unprotected key data.

The identifier of the VMK should match the identifier in the BEK file header.

Appendix A. References

[FERGUSON06]
Title: AES-CBC + Elephant diffuser - A Disk Encryption Algorithm for Windows Vista
Author(s): Niels Ferguson
Date: August 2006
URL: http://download.microsoft.com/download/0/2/3/0238acaf-d3bf-4a6d-b3d6-0a0be4bbb36e/bitlockercipher200608.pdf

[KUMAR08]
Title: Bitlocker and Windows Vista
Author(s): Nitan Kumar, Vipin Kumar
Date: May 19, 2008
URL: http://www.nvlabs.in/nvbit_bitlocker_white_paper.pdf

[KORNBLUM09]
Title: Implementing BitLocker Drive Encryption for Forensic Analysis
Author(s): Jesse Kornblum
Date: 2009
URL: http://jessekornblum.com/publications/di09.pdf

[KORNBLUM10]
Title: BitLocker To Go
Author(s): Jesse Kornblum
Date: 2010
URL: http://jessekornblum.com/presentations/dodcc10-1.pdf

[MSDN]
Title: BitLocker Drive Encryption Overview
URL: http://technet.microsoft.com/en-us/library/cc732774.aspx

Appendix B. GNU Free Documentation License

Version 1.3, 3 November 2008

0. PREAMBLE

The purpose of this License is to make a manual, textbook, or other functional and useful document "free" in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or noncommercially. Secondarily, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of "copyleft", which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

1. APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The "Document", below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as "you". You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A "Modified Version" of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A "Secondary Section" is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The "Invariant Sections" are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The "Cover Texts" are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A "Transparent" copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not "Transparent" is called "Opaque".

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The "Title Page" means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, "Title Page" means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.

The "publisher" means any person or entity that distributes copies of the Document to the public.

A section "Entitled XYZ" means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as "Acknowledgements", "Dedications", "Endorsements", or "History".) To "Preserve the Title" of such a section when you modify the Document means that it remains a section "Entitled XYZ" according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

2. VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

3. COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

4. MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

- A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.
- B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.
- C. State on the Title page the name of the publisher of the Modified Version, as the publisher.
- D. Preserve all the copyright notices of the Document.
- E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.
- F. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.
- G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.
- H. Include an unaltered copy of this License.
- I. Preserve the section Entitled "History", Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.
- J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years before the Document

itself, or if the original publisher of the version it refers to gives permission.

- K. For any section Entitled "Acknowledgements" or "Dedications", Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.
- L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.
- M. Delete any section Entitled "Endorsements". Such a section may not be included in the Modified Version.
- N. Do not retitle any existing section to be Entitled "Endorsements" or to conflict in title with any Invariant Section.
- O. Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.

You may add a section Entitled "Endorsements", provided it contains nothing but endorsements of your Modified Version by various parties—for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

5. COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled "History" in the various original documents, forming one section Entitled "History"; likewise combine any sections Entitled

"Acknowledgements", and any sections Entitled "Dedications". You must delete all sections Entitled "Endorsements".

6. COLLECTIONS OF DOCUMENTS
You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

7. AGGREGATION WITH INDEPENDENT WORKS
A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an "aggregate" if the copyright resulting from the compilation is not used to limit the legal rights of the compilation's users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document's Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

8. TRANSLATION
Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled "Acknowledgements", "Dedications", or "History", the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

9. TERMINATION
You may not copy, modify, sublicense, or distribute the Document except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, or distribute it is void, and will automatically terminate your rights under this License.

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, receipt of a copy of some or all of the same material does not give you any rights to use it.

10. FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See http://www.gnu.org/copyleft/.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License "or any later version" applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation. If the Document specifies that a proxy can decide which future versions of this License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Document.

11. RELICENSING

"Massive Multiauthor Collaboration Site" (or "MMC Site") means any World Wide Web server that publishes copyrightable works and also provides prominent facilities for anybody to edit those works. A public wiki that anybody can edit is an example of such a server. A "Massive Multiauthor Collaboration" (or "MMC") contained in the site means any set of copyrightable works thus published on the MMC site.

"CC-BY-SA" means the Creative Commons Attribution-Share Alike 3.0 license published by Creative Commons Corporation, a not-for-profit corporation with a principal place of business in San Francisco, California, as well as future copyleft versions of that license published by that same organization.

"Incorporate" means to publish or republish a Document, in whole or in part, as part of another Document.

An MMC is "eligible for relicensing" if it is licensed under this License, and if all works that were first published under this License somewhere other than this MMC, and subsequently incorporated in whole or in part into the MMC, (1) had no cover texts or invariant sections, and (2) were thus incorporated prior to November 1, 2008.

The operator of an MMC Site may republish an MMC contained in the site under CC-BY-SA on the same site at any time before August 1, 2009, provided the MMC is eligible for relicensing.