Reference Manual
of
Vendor Specific Extensions
of
WD My Passport drive

Rev. D, 06.07.2016

----

* INFORMATIONS ARE PROVIDED ``AS IS'' AND ANY EXPRESS OR IMPLIED
* WARRANTIES ARE DISCLAIMED. IN NO EVENT NO ONE THAN YOU WILL BE LIABLE
* FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
* CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, LOSS OF DATA)
* ARISING IN ANY WAY OUT OF THE USE OF INFORMATIONS IN THIS DOCUMENT

Informations provided herein are compiled from various information source and/or based on observation. They are not derived from an oficial vendor documentation nor they has been verified by vendor. They has been tested on very limited test of devices.

!!!!!!!!!!!!!!!!!!!!!!!!!!!!! DANGER !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Use of command described here may cause irrepairable lost of drive content.
!!!!!!!!!!!!!!!!!!!!!!!!!!!!! DANGER !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

===

1. *** VENDOR SPECIFIC SCSI COMMANDS

===

1.1 ENCRYPTION STATUS(10) command

The ENCRYPTION STATUS(10) command (see table 1) requests that information regarding current security/encryption status of server device to be sent to an application client. For the format of returned data see table 2.

Table 1 - ENCRYPTION STATUS(10) command

B \ b	7	6	5	4	3	2	1	0
0	OPERATION CODE (C0h)							
1	OPERATION SUBCODE (45h)							
2	Reserved							
6								
7	(MSB) ALLOCATION LENGTH							
8								(LSB)
9	CONTROL							

ALLOCATION LENGTH field

The Allocation length should be at least 16B, so that NUMBER OF CIPHERS is returned.

Table 2 - ENCRYPTION STATUS data format

B \ b	7	6	5	4	3	2	1	0
0	SIGNATURE (45h)							
1	Reserved							

2	
3	SECURITY STATUS
4	CURRENT CIPHER ID
5	Reserved
6	(MSB) PASSWORD LENGTH
7	(LSB)
8	KEY RESET ENABLER
11	
12	Reserved
14	
15	NUMBER OF CIPHERS
16	CIPHER 0
15+n	CIPHER n

SIGNATURE field

The SIGNATURE field is 45h all the times

SECURITY STATUS field

The SECURITY STATUS field report the current security status of server device. The values are described in table 3.

Table 3 - SECURITY STATUS

Status	Description
0	Device encryption key is not protected by user supplied password
1	Device encryption key is locked
2	Device encryption key is user password protected and unlocked
6	As [1] but no more unlock attempts are allowed
7	Device has no encryption key
Status 0 mean that data are still encrypted on the drive, but encryption key is scrambled by a vendor specific default password (see bellow). Default password needs not to be supplied by application to unlock drive on boot - the drive will enter mode 0 automatically Device with user password set starts in mode 1, see UNLOCK ENCRYPTION command for more information Device with no encryption key (mode 7) should not be seen in production	

Note the vendor specific default password mentioned in Table 3 is:

```
AES-256: 03 14 15 92 65 35 89 79 32 38 46 26 43 38 32 79
         FC EB EA 6D 9A CA 76 86 CD C7 B9 D9 BC C7 CD 86

AES-128: 03 14 15 92 65 35 89 79 2B 99 2D DF A2 32 49 D6
```

CURRENT CIPHER ID

The CURRENT CIPHER ID field report the encryption alghoritm used on device. Possible values are described in table 4.

Table 4 - CIPHER ID

ID	Cipher Alghoritm
00h	No encryption
10h	AES 128 ECB
12h	AES 128 CBC
18h	AES 128 XTS
20h	AES 256 ECB
22h	AES 256 CBC
28h	AES 256 XTS
30h	Full Disc Encryption (FDE)

Note the 1xh and 2xh encryption is handled by USB<->SATA bridge chip. FDE mean the encryption is handled by HDD itself (USB<->SATA bridge is just pure bridge).

PASSWORD LENGTH field

The PASSWORD LENGTH field contain the length of password used on drive. Password is binary blob of specified size. The size is expressed in bytes. It is 16B for AES 128 cipher suite and 32B for AES 256 cipher suite and FDE.

KEY RESET ENABLER field

The KEY RESET ENABLER field is four byte code required for subsequent RESET DATA ENCRYPTION KEY command. Such command needs to be called immediatelly as code changes with any command issued on device.

NUMBER OF CIPHERS and CIPHER n

The NUMBER OF CIPHERS and CIPHER n fields describe th elist of encryption alghoritms supported by the device. For description of CIPHER i field see table 4.

===

1.2 UNLOCK ENCRYPTION(10) command

The UNLOCK ENCRYPTION(10) command (see table 5) provides a means for an application to supply the password that unlock the drive encryption key.

The security status needs to be 1 (LOCKED, see table 3) otherwise command will be terminated with CHECK CONDITION status, with sense key set to ILLEGAL REQUEST, and additional sense code set to 74h/81h (if security status 0, 2 or 7) or 74h/80h (if security status 06h).

If security status is 1, the supplied password is used to unlock internal encryption key. For the format of command parameter block see table 6.

If unlock attempt is unsuccesfull, command will be terminated with CHECK CONDITION status, with sense key set to ILLEGAL REQUEST, and additional sense code set to AUTHENTICATION FAILED (74h/40h). Number of unsuccesfull attempt is incremented.

If number of unsucesfull attempts exceed an internal limit, secure status become 6 and no further unlock attempts are allowed. Either power off/on transition or RESET DATA ENCRYPTION KEY is required to solve it.

On succesfull unlock the security status of device become 2 (UNLOCKED) .

Unless unlocked, access to most common commands including reading and writting a sector of drive or format is not allowed. Those commands are terminated with CHECK CONDITION status, with sense key set to DATA PROTECT, and additional sense code set to LOGICAL UNIT ACCESS NOT AUTHORIZED (74h/71h).

Table 5 - UNLOCK ENCRYPTION(10) command

B \ b	7	6	5	4	3	2	1	0
0	OPERATION CODE (C1h)							
1	OPERATION SUBCODE (E1h)							
2	Reserved							
6								
7	(MSB) PARAMETER LIST LENGTH							
8								(LSB)
9	CONTROL							

PARAMETER LIST LENGTH field

The Parameter list length need to follow exact size of expected parameter block size of command will be terminated with CHECK CONDITION status, with sense key set to ILLEGAL REQUEST, and additional sense code set to INVALID FIELD IN CDB (24h/00h).

Table 6 - UNLOCK ENCRYPTION data format

B \ b	7	6	5	4	3	2	1	0
0	SIGNATURE (45h)							
1	Reserved							
5								
6	(MSB) PASSWORD LENGTH							
7								(LSB)
8	PASSWORD							
8+L								

SIGNATURE field

The SIGNATURE field is 45h all the times

PASSWORD LENGTH and PASSWORD fields

The PASSWORD LENGTH field contain the length of password used on drive. The size is expressed in bytes. PASSWORD field is binary blob of specified size. The size is expressed in bytes.

The size of password is not user selectable it must be exactly the same as specified by the drive in PASSWORD LENGTH field of response to ENCRYPTION STATUS command or command will be terminated with CHECK CONDITION status, with sense key set to ILLEGAL REQUEST, and additional sense code set to INVALID FIELD IN PARAMETER LIST (26h/00h).

===

1.3 CHANGE ENCRYPTION PASSPHRASE(10) command

The CHANGE ENCRYPTION PASSPHRASE(10) command (see table 7) provides a means for an application to change the password that unlock the drive encryption key. It can be used to enable and disable password security as well.

"Disabled password security" mean that security status is 0 and password needs not to be supplied by application to access the drive. See table 3 for more information.

The security status needs to be 2 (UNLOCKED, see table 3) for password change and disable security operations and 0 (NotProtected) for enable security operation. If drive is not in expected state the command will be terminated with CHECK CONDITION status, with sense key set to ILLEGAL REQUEST, and additional sense code set to 74h/81h (if security status 0, 2 or 7) or 74h/80h (if security status 06h).

For password change and disable security operations the old password is required. If password is not correct, command will be terminated with CHECK CONDITION status, with sense key set to ILLEGAL REQUEST, and additional sense code set to AUTHENTICATION FAILED (74h/40h). Number of unsuccesfull attempt is incremented.

If number of unsucesfull attempts exceed an internal limit, drive's secure status become 6 and no further change encryption passphrase nor unlock attempts are allowed. Either power off/on transition or RESET DATA ENCRYPTION KEY is required to solve it.

For the format of command parameter block see table 8.

If old password is correct or "enable security" operation is requested, the new password si installed in the drive. Security status of device become 2 (UNLOCKED) for password change and enable security operations or 0 (NotProtected) for disable security operation.

Table 7 - CHANGE ENCRYPTION PASSPHRASE(10) command

B \ b	7	6	5	4	3	2	1	0
0	OPERATION CODE (C1h)							
1	OPERATION SUBCODE (E2h)							
2	Reserved							
6								
7	(MSB) PARAMETER LIST LENGTH							
8								(LSB)
9	CONTROL							

PARAMETER LIST LENGTH field

The Parameter list length need to follow exact size of expected parameter block size of command will be terminated with CHECK CONDITION status, with sense key set to ILLEGAL REQUEST, and additional sense code set to INVALID FIELD IN CDB (24h/00h).

Table 8 - CHANGE ENCRYPTION PASSPHRASE data format

B \ b	7	6	5	4	3	2	1	0
0	SIGNATURE (45h)							

```
|   1  |                                                              |
+------+-------                 Reserved                     ------+
|   2  |                                                              |
+------+-------+-------+------+-------+------+-------+------+-------+
|   3  |       Reserved       | NEWDEF|       Reserved       | OLDDEF|
+------+-------+-------+------+-------+------+-------+------+-------+
|   4  |                                                              |
+------+-------                 Reserved                     ------+
|   5  |                                                              |
+------+-------+------+-------+------+-------+------+-------+------+-------+
|   6  | (MSB)                                                        |
+------+-------              PASSWORD LENGTH                  ------+
|   7  |                                                       (LSB) |
+------+-------+------+-------+------+-------+------+-------+------+-------+
|   8  |                                                              |
+------+-------                OLD PASSWORD                   ------+
| 7+L  |                                                              |
+------+-------+------+-------+------+-------+------+-------+------+-------+
| 8+L  |                                                              |
+------+-------                NEW PASSWORD                   ------+
| 7+2*L|                                                              |
+------+-------+-------+------+-------+------+-------+------+-------+
```

SIGNATURE field

The SIGNATURE field is 45h all the times

OLDDEF bit

The OLDDEF bit is set to 1 then OLD PASSWORD content is ignored and vendor specific default password is used instead. It is used for "enable security" operation.

NEWDEF bit

The NEWDEF bit is set to 1 then NEW PASSWORD content is ignored and vendor specific default password is used instead. It is used for "disable security" operation. Both NEWDEF and OLDDEF must not be set to 1 at the same time or command will be terminated with CHECK CONDITION status, with sense key set to ILLEGAL REQUEST, and additional sense code set to INVALID FIELD IN PARAMETER LIST (26h/00h).

PASSWORD LENGTH, OLD PASSWORD and NEW PASSWORD fields

The PASSWORD LENGTH field contain the length of password used on drive. The size is expressed in bytes. OLD PASSWORD and NEW PASSWORD fields are binary blob of specified size. The size is expressed in bytes.

The size of password is not user selectable it must be exactly the same as specified by the drive in PASSWORD LENGTH field of response to ENCRYPTION STATUS command or command will be terminated with CHECK CONDITION status, with sense key set to ILLEGAL REQUEST, and additional sense code set to INVALID FIELD IN PARAMETER LIST (26h/00h).

 ==

1.4 RESET DATA ENCRYPTION KEY(10) command

The RESET DATA ENCRYPTION KEY(10) command (see table 9) enforce drive to install new Data Encryption Key (DEK). It doesn't change data stored on the medium, but they can't be decrypted anymore as old encryption key become lost.

Some drives use provided KEY to derive DEK from it. The KEY may become DEK as supplied, or it's XORed by random value (generated by drive itself) first. Some drives use no user supplied KEY for DEK generation.

Command can be called in any security state. It's intended to solve "lost user password" condition or change internal encryption alghoritm or just to quickly make all data on medium inaccesible.

User password become deleted (replaced by vendor specific default password; see note bellow table 3).

Security state of device become 0 (NotProtected).

Reset Data Encryption Key command is protected against unintended invocation by KEY RESET ENABLER field. The ENCRYPTION STATUS command needs to be called just before RESET DATA ENCRYPTION KEY command to obtain valid code (see table 2). If no valid code filled then command will be terminated with CHECK CONDITION status, with sense key set to ILLEGAL REQUEST, and additional sense code set to INVALID FIELD IN CDB (24h/00h).

For the format of command parameter block see table 10.

Table 9 - RESET DATA ENCRYPTION KEY(10) command

B \ b	7	6	5	4	3	2	1	0
0	OPERATION CODE (C1h)							
1	OPERATION SUBCODE (E3h)							
2	KEY RESET ENABLER							
5								
6	Reserved							
7	(MSB) PARAMETER LIST LENGTH							
8								(LSB)
9	CONTROL							

PARAMETER LIST LENGTH field

The Parameter list length need to follow exact size of expected parameter block size of command will be terminated with CHECK CONDITION status, with sense key set to ILLEGAL REQUEST, and additional sense code set to INVALID FIELD IN CDB (24h/00h).

Table 10 - RESET DATA ENCRYPTION KEY data format

B \ b	7	6	5	4	3	2	1	0
0	SIGNATURE (45h)							
1	Reserved							
2								
3	Reserved							COMBINE
4	CIPHER ID							
5	Reserved							
6	(MSB) KEY LENGTH							
7								(LSB)
8	KEY							
7+L								

SIGNATURE field

The SIGNATURE field is 45h all the times

COMBINE bit

If 0 the KEY is used as-is.
If 1 all bytes of KEY are XORed with output of drive's internal random number generator before further use.

Some drives (FDE?) may not support COMBINE=1.

CIPHER ID field

The drive's data encryption alghoritm will be set to the one specified by ID. List of supported ciphers can be found in response to ENCRYPTION STATUS command, see table 2 and table 4 for description.

KEY LENGTH and KEY fields

The KEY LENGTH field contain the length of KEY blob. The size is expressed in bites (not bytes as in password length used in other commands).

On some drives the KEY supplied become new DEK (but remember COMBINE bit effect). On some drives (FDE?) use no KEY supplied, drive will generate new DEK by self.

The size of data is not user selectable it must be same as the password length of password of selected CIPHER ID. Otherwise command will be terminated with CHECK CONDITION status, with sense key set to ILLEGAL REQUEST, and additional sense code set to INVALID FIELD IN PARAMETER LIST (26h/00h).

1.5 READ HANDY CAPACITY(10) command

The READ HANDY CAPACITY(10) command (see table 11) return the parameters of drive's handy store. Handy store is data store independent from main drive capacity. The applications may read and write data here according own requirements. Stored data has no meaning for drive itself. Handy Store data can be read in any security state. It can be written in unlocked or not protected state only.

For the format of returned data see table 12.

Table 11 - READ HANDY CAPACITY(10) command

B \ b	7	6	5	4	3	2	1	0
0	OPERATION CODE (D5h)							
1	Reserved							
8								
9	CONTROL							

Table 12 - READ HANDY CAPACITY data format

B \ b	7	6	5	4	3	2	1	0
0	(MSB)	LAST HANDY BLOCK ADDRESS						
3								(LSB)
4	(MSB)	BLOCK LENGTH						
7								(LSB)

8	Reserved							
9								
10	(MSB) MAXIMUM TRANSFER LENGTH							
11								(LSB)

LAST HANDY BLOCK ADDRESS field

The LAST HANDY BLOCK ADDRESS field contain the address of last addressable handy store block.

BLOCK LENGTH field

The BLOCK LENGTH field contain the size (in bytes) of a handy store block.

MAXIMUM TRANSFER LENGTH

The MAXIMUM TRANSFER LENGTH field contain the maximum number of blocks that can be read/written at once.

==

1.6 READ HANDY STORE(10) command

The READ HANDY STORE(10) command (see table 13) request that device read the specified handy store block and transfer them to the data-in buffer.

See READ HANDY CAPACITY command for more description of Handy Store

Table 13 - READ HANDY STORE(10) command

B \ b	7	6	5	4	3	2	1	0
0	OPERATION CODE (D8h)							
1	Reserved							
2	(MSB) HANDY STORE BLOCK ADDRESS							
5								(LSB)
6								
7	(MSB) TRANSFER LENGTH							
8								(LSB)
9	CONTROL							

HANDY STORE BLOCK ADDRESS field

The HANDY STORE BLOCK ADDRESS field specifies first handy store block accesed by this command.

TRANSFER LENGTH field

The TRANSFER LENGTH field specifies number of contiguous handy store blocks of data that shall be read and transferred to the data-in buffer, starting with the handy store block specified by HANDY STORE BLOCK ADDRESS field.

==

1.7 WRITE HANDY STORE(10) command

The WRITE HANDY STORE(10) command (see table 14) request that device transfer the specified handy store block(s) from the data-out buffer and write them.

See WRITE HANDY CAPACITY command for more description of Handy Store

Table 14 - WRITE HANDY STORE(10) command

B \ b	7	6	5	4	3	2	1	0
0	OPERATION CODE (DAh)							
1	Reserved							
2	(MSB)	HANDY STORE BLOCK ADDRESS						
5								(LSB)
6								
7	(MSB)	TRANSFER LENGTH						
8								(LSB)
9	CONTROL							

HANDY STORE BLOCK ADDRESS field

The HANDY STORE BLOCK ADDRESS field specifies first handy store block accesed by this command.

TRANSFER LENGTH field

The TRANSFER LENGTH field specifies number of contiguous handy store blocks of data that shall be transferred from data-out buffer and written, starting with the handy store block specified by HANDY STORE BLOCK ADDRESS field.

===

2. *** VENDOR SPECIFIC MODE PAGES

===

2.1 Device Configuration Page (20h)

The Device Configuration Page for MODE SENSE/MODE SELECT defines device configuration parameters.

Table 15 - Device Configuration Page (20h)

B \ b	7	6	5	4	3	2	1	0
0	PS	Reserved	PAGE CODE (20h)					
1	PAGE LENGTH (06h)							
2	SIGNATURE (30h)							
3	Reserved							
4	DisAP	Reserved					DisCD	DisSES
5	Reserved						2TBL	DisWL
6	Reserved							
7								

PS (Parameter Savable) bit

The returned Parameter Savable (PS) bit of 1 indicates that page 01h parameter data is savable.

DisAP (Disable AP), DisWL (Disable White List) bits

The meaning of Disable AP and Disable White List is unknown

DisCD (Disable CDROM), DisSES (Disable SES) bits

Setting appropriate bits to 1 disable emulated CDROM device and/or SES device.

2TBL (Two TB Limit)

Setting the bit to 1 limit reported drive capacity to 2TB maximum.

===

2.2 Operations Page (21h)

The Operations Page for MODE SENSE/MODE SELECT defines device operation parameters.

Table 16 - Operations Page (21h)

B \ b	7	6	5	4	3	2	1	0
0	PS	Reserved	PAGE CODE (21h)					
1	PAGE LENGTH (0Ah)							
2	SIGNATURE (30h)							
3	Reserved							
4	Reserved						LOOSESB2	ESATA15
5	Reserved						CDMValid	ENCDEJ
6	Reserved							
7								
8	POWER LED BRITE							
9	BACKLIGHT BRITE							
10	Reserved							INVLCD
11	Reserved							

PS (Parameter Savable) bit

The returned Parameter Savable (PS) bit of 1 indicates that page 01h parameter data is savable.

LOOSESB2 (Loose SB2) bit

The meaning of Loose SB2 bit is unknown. It seems to be related to Fibre Channel - Single-Byte Command Code Sets Mapping Protocol - 2. (FC-SB-2)

ESATA15 (eSATA15) bit

The meaning of eSATA15 bit is unknown. It may be related to speed on eSATA port (150MBps)

CDMValid (CD Media Valid), ENCDEJ (Enable CD Eject) bits

The meaning of both of CD Media Valid and Enable CD Eject bits is unknown.

POWER LED BRITE and BACKLIGHT BRITE values

The POWER LED BRITE and BACKLIGHT BRITE values control the brigthness of power LED and LCD display backlight.

INVLCD (Inverted LCD) bit

The Inverted LCD bit turn LCD display to be negative (white on black).

===

2.3 Return All Pages Page (3Fh)

Note that standard MODE SENSE Return All Pages command seems to have off-by-one bug in some firmware versions. It report +1 size on list of returned pages, so the latest reported page is random number. It doesn't affect common drive operations in any way.

===

3. *** WD UTILITIES specific API (software)

===

The drive itself use password in the form of binary blob of fixed length (16B for AES 128 ciphers, 32B for AES 256 ciphers and FDE). It's necesarry to transform user's text input into that form. Such transform needs to be consistent accross utilities or resulting password blob will not be same and unlock operation will fail. Current WD Utilities use salted sha256 hash to compute password blob from user input for AES 256 and FDE. AES 128 drives are unsupported by current version of WD Utilities, so WD standard alghoritm is not known for AES 128 suite.

All string operations (e.g. user input and hash) are done in UCS-2 (little-endian) encoding.

The pseudo code of alghoritm used in WD Utilities:

```
1. STR = CONCAT(SALT, UPW)
2. FOR i=1 TO i==ITERATION_COUNT DO STR = sha256Digest(STR)
3. RETURN (STR)
```

Where UPW is password as entered by user
SALT is salt prepended to such password for the purpose of digest calculation
ITERATION_COUNT is the number of times the sha256Digest is applied to string

On exit STR contain password blob used for password operations on drive

Based on exact version and platform of WD Utilities, the SALT and ITERATION_COUNT are either hardcoded in the code or stored in Security Block (drive's Handy Store block 1). In the first case, the SALT of "WDC." is used and ITERATION COUNT is 1000. In the second case, stored data are used for password blob calculation. Vendor specific READ HANDY STORE(10) command should be used to read Security Block from drive. Hardcoded default Salt and Iteration Count will be used if no Security Block found on drive.

Even if stored SALT and ITERATION COUNT are honored by WD utilities for the purpose of password blob calculation, they are rewritten to defaults on first password change.

3.1 Security Block (drive's Handy Store block 1)

For the description of format of Security Block (drive's Handy Store block 1) see table 17.

Table 17 - Security Block (Handy Store block 1)

B	
0 3	SIGNATURE (00h 01h 'W' 'D')
4-7	Reserved
8-12	(MSB) ITERATION COUNT (LSB)
12-19	SALT
20-23	Reserved
24-225	HINT
226-510	Reserved
511	CHECKSUM

ITERATION COUNT field

The Interation Count field hold the number of digest operation applied on salted user password string.

SALT and HINTS fields

The SALT and HINTS fields are UCS-2 little endian encoded strings. The first one is uset as salt in process of password blob calculation. The second one is just hint for the user to help him to enter password. Such arbitrary string has no meaning for drive nor WD utilities beyond it can be displayed to user.

CHECKSUM field

The CHECKSUM field is used to verify the validity of the block. Sum of all bytes in the block needs to be zero or block is considered invalid. Note that it seems that some version of WD utilities count first byte of sector twice as accident. As it is 0x00 it doesn't broke the result

NOTE 1: Hardware is not tied to alghoritm used by WD Utilities nor the content of Handy Store Block 1 (Security Block). It's possible to implement different alghoritm and maintain the drive using it. Of course, vendor's WD utilities will not be able to maintain such disc at the same time.

NOTE 2: Alghoritm described above is used on drives set to AES 256 suite of ciphers and for FDE. AES 128 suite is not supported by current WD utilities, thus there is no "standard vendor alghoritm" used to calculate password blob known for such drives.

3.2 User Block (drive's Handy Store block 2)

Independent device label can be set and is recognized by WD Utilities in User Block (Handy Store Block 2). For format of such block see table 18. Vendor specific READ HANDY STORE(10) command should be used to read User Block from drive.

Table 18 - User Block (Handy Store block 2)

B	
0	SIGNATURE (00h 02h 'W' 'D')
3	
4-7	Reserved
8-71	LABEL
72-510	Reserved
511	CHECKSUM

LABEL field

The LABEL field is UCS-2 little endian encoded strings. It is used as device label.

CHECKSUM field

See table 17 for description.

==

4. *** Security notes

==

a) Drive is shipped with vendor generated DEK. The quality of such key is known to be low, it can be guessed. Remember, change of User Password doesn't change the DEK. Always call RESET DATA ENCRYPTION KEY on new drive to replace manufacturers DEK by new one.

Unfortunatelly, KEY provided by vendor's utility has also very low entropy and even drive's internal RNG is very poor, so even DEK generated by vendor's utility have low quality. Use own utility to reset key (provide high quality cryptography KEY on input). If not possible to use own utility, prefer FDE flavor of drives.

b) Due design bug it's possible to acccess some kind of drive even with *previous* user password, not just the most recent one. Remember, unlocked drive mean it's locked by well known password, so if you protect unprotected buggy drive, it still can be unlocked by previous (well known) password. Always change user password twice when locking unlocked drive (or when replacing disclosed password).

c) So many other bugs and backdoors has been discovered for those drives. To be on safe side, never assume the drive content is safe against skilled attacker, regardless of the claimed encryption. Some kind of attacks require neither special equipment nor high computing power.

Search for following paper for more details.

----

got HW crypto ?
On the (in)security of a Self-Encrypting Drive series

Authors: Gunnar Alendal, Christian Kison, modg
