

ATA Security feature Set Clarifications

To: T13 Technical Committee
From: Jim Hatfield
Seagate Technology
(with Jeff Wolford: Hewlett-Packard)
389 Disc Drive
Longmont, CO 80503
Phone: 720-684-2120
Fax: 720-684-2722
Email: James.C.Hatfield@seagate.com
Date: February 6, 2006

Revision History:

- 0: Initial revision
- 1: Incorporate feedback from Dec. 2005 plenary. Split the Enhancements to a separate proposal.

Introduction

The purpose of this proposal is to clarify a number of vague and unspecified issues regarding the ATA Security Mode feature set. This is the source of unpredictable behavior between vendors and models currently in the market. Locking down the specification of ATA Security is critical to ensuring reliable interoperability.

Proposal

I propose that the following text be incorporated into ATA/ATAPI-8 ACS.

1.1 Security Mode feature set

The optional Security Mode feature set is a password system that restricts access to user data stored on a device. In addition, access to some configuration capabilities is restricted.

See also the '~~Master Password Revision Code~~Master Password Identifier' feature (1.2) and '~~Enhanced Security Mode feature set~~' (1.3) which are is an optional enhancements to the Security Mode feature set.

1.1.1 Security attributes

These are the Security attributes:

- Power: on or off
- Feature set supported: True or False _____ (see 1.1.6)
- Locked: True or False _____ (see 1.1.2)
- Security Level: High or Maximum _____ (see 1.1.3)
- Attempt Limit counter _____ (see 1.1.9)
- Frozen: True or False _____ (see 1.1.4)
- User password _____ (see 1.1.2)
- Master password _____ (see 1.1.2)
- Master Password Identifier (see 1.2)

Here are some special terms used in the Security Mode feature set:

<u>Security Not Supported</u>	<u>The Security feature set is not supported. The security commands (see 1.1.5) are not supported and shall be command aborted.</u>
Security Disabled	The Security Mode feature set is supported, but that there is no valid User password. There is a Master password. Access to user data is not restricted by the Security Mode feature set. The terms 'Security Locked' and 'Security Unlocked' are not applicable.
Security Enabled	The Security Mode feature set is supported, and a valid User password has been set.
Security Locked	Security is enabled. In addition, all access to user data is denied.
<u>Security Unlocked</u>	<u>Security is enabled. A SECURITY UNLOCK command was successful. In addition, access to user data is not restricted by the Security feature set.</u>
<u>Security Level</u>	<u>A 'High' security level unlocks with either Master or User valid</u>

	<u>password. A 'Maximum' security level unlocks only with a valid User password</u>
Security Retries Expired	Too many commands attempted to use an incorrect password. Further password accesses are denied until a power-on or hardware reset.
Security Frozen	Security may be either enabled or disabled. Changes to Security attributes are not allowed until after the next power on reset.

1.1.2 Master and User Passwords

The system has two passwords, User (~~optional~~) and Master (~~required~~), and two security levels, High and Maximum.

1.1.2.1 User Password and Locking

The purpose of the User password is to create a lock to prevent unauthorized access to any user data on the device. The User password may be used to unlock the device to allow authorized access to data.

The security system is enabled by ~~sending a user setting a User password to the device~~ with the SECURITY SET PASSWORD command. When the security system is enabled, the device is automatically Locked (e.g. access to user data on the device is denied) after a power cycle until the User password is sent to the device with the SECURITY UNLOCK command.

1.1.2.2 Master Password

The purpose of the Master password is to allow an administrator to establish a password that is kept secret from the user, and which may be used to unlock the device if the User password is lost.

~~A device always has a Master password. A factory-installed Master password may be valid before an initial SECURITY SET (master) PASSWORD command has been successfully executed. A~~ The Master password may be ~~set~~ used in addition to the User password. ~~The purpose of the Master password is to allow an administrator to establish a password that is kept secret from the user, and which may be used to unlock the device if the User password is lost. Setting the Master password does not enable the password~~ Security system (e.g. does not Lock the device).

1.1.3 High and Maximum Security Level

A device with Security enabled has two levels of security: High or Maximum.

The security level is set to “High” or “Maximum” with the SECURITY SET PASSWORD command. The security level determines device behavior when the Master password is used-with the SECURITY DISABLE PASSWORD, SECURITY UNLOCK and SECURITY ERASE UNIT commands ~~to unlock the device.~~

When the security level is set to High, either the User or Master password may be used. ~~the device requires the SECURITY UNLOCK command and the Master password to unlock.~~ See This is the highest level of security available. Table 1 . This provides a level of security between None and Maximum.

When the security level is set to Maximum, the Master password cannot be used with the SECURITY DISABLE PASSWORD and SECURITY UNLOCK commands. The SECURITY ERASE UNIT command, however, does accept the either the User or Master password. ~~the device requires a SECURITY ERASE PREPARE password. command and a SECURITY ERASE UNIT command with the masterpassword to unlock. Execution of the SECURITY ERASE UNIT command erases all user data on the device. This is the highest level of security available.~~

Table 1 - Interaction of Security Levels and Passwords

Security Level	Pswds Existing	Pswd Supplied	Action Resulting from Commands		
			SECURITY DISABLE PASSWORD	SECURITY UNLOCK	Properly Prefaced SECURITY ERASE UNIT
Disabled	master only	master (correct)	N	N	E
Disabled	master only	user (not valid)	A	A	A
High	master and user	master (correct)	E	E	E
High	master and user	user (correct)	E	E	E
Maximum	master and user	master (correct)	A	A	E
Maximum	master and user	user (correct)	E	E	E

Key:

- N** Nop – Do nothing, but return normal completion.
- A** Return command aborted
- E** Execute the command (if all other validations pass); otherwise return command aborted.

1.1.4 Frozen Mode

The SECURITY FREEZE LOCK command prevents changes to passwords all Security attributes until a following power cycle or hardware reset. The purpose of the SECURITY FREEZE LOCK command is to prevent password setting attacks on the security system.

[Editors note: This section conflicts with **Figure 1**, (transitions SEC2:SEC1, and SEC6:SEC4), and with section 1.11) How to resolve it ? The stated precedence is Tables, Figures, and then text. The Figure allows Hardware reset to clear the Freeze Lock, but it is within the text that the conflict exists. So, the text must be made to agree with the Figure.]

1.1.5 Commands

A device that implements the Security Mode feature set shall implement the following minimum set of commands:

- SECURITY SET PASSWORD
- SECURITY UNLOCK
- SECURITY ERASE PREPARE
- SECURITY ERASE UNIT
- SECURITY FREEZE LOCK
- SECURITY DISABLE PASSWORD

1.1.6 IDENTIFY DEVICE data

Support of the Security Mode feature set is indicated in IDENTIFY DEVICE and IDENTIFY PACKET DEVICE data word 82 and data word 128.

Security information in words 82, 89 and 90 is fixed until the next power-on reset and shall not change unless DEVICE CONFIGURATION OVERLAY removes support for the Security Mode feature set.

Security information in words ~~82~~, 85, 92 and 128 are variable and may change.

If the Security Mode feature set is not supported, then words 89, 90, 92 and 128 are ~~invalid N/A and shall be cleared to zero.~~ should be ignored by the host.

1.1.7 Security mode initial setting

When the device is shipped by the manufacturer, the state of the Security Mode feature shall be disabled (e.g. is not Locked). The initial Master password value is not defined by this standard.

~~If the Master Password Revision Code feature is supported, the Master Password Revision Code shall be set to FFFFh by the manufacturer.~~

1.1.8 ~~User password lost~~ Password Rules

This section applies to any Security command that accepts a password, and for which there exists a valid password. ~~This section does not apply while Security is Frozen.~~

If Security is disabled and there is a valid Master password, then the Master password may be used.

The SECURITY ERASE UNIT command ignores the Security Level attribute when comparing passwords, and shall accept a valid Master or User password.

If the User password sent to the device ~~with the SECURITY UNLOCK command~~ does not match the user password previously set with the SECURITY SET PASSWORD command, the device shall ~~not allow the user to access data~~ return command aborted.

If the Security Level was set to High during the last SECURITY SET (user) PASSWORD command, the device shall ~~unlock~~ if accept the Master password ~~is received~~ and complete normally.

If the Security Level was set to Maximum during the last SECURITY SET (user) PASSWORD command, the device shall ~~not unlock~~ return command aborted if the Master password is ~~received~~ supplied. ~~The~~ However, the SECURITY ERASE UNIT command, shall erase all user data and shall unlock the device if the Master password matches the last Master password previously set with the SECURITY SET PASSWORD command.

1.1.9 Attempt limit for SECURITY UNLOCK command

The device shall have an attempt limit counter. The purpose of this counter is to defeat repeated trial attacks. After each failed User or Master password SECURITY UNLOCK command, the counter is decremented. Once the counter reaches zero, it shall not be decremented, and ~~When the counter value reaches zero~~ the EXPIRE bit (bit 4) of IDENTIFY DEVICE data word 128 ~~is~~ shall be set to one, and the SECURITY UNLOCK and SECURITY UNIT ERASE commands ~~are~~ shall be command aborted until the device is powered off or hardware reset. The EXPIRE bit shall be cleared to zero after power-on or hardware reset. The counter shall be set to five after a power-on or hardware reset.

1.1.10 Resets

When Software Reset and Device Reset occurs between commands, the device shall not change any Security attribute of the device.

Hardware Reset behavior may be affected by the ‘Software Settings Preservation’ (SSP) feature described in SATA-IO document “Serial ATA Revision 2.5”.

Power-on Reset causes an exit from Frozen mode and preserves any Master and User passwords that have been set. The device shall enter ~~either~~ security state SEC1 ~~or~~ SEC4 ~~depending on whether~~ if Security is disabled or SEC4 if Security is enabled.

If aAny reset or power-down event that occurs during the execution of a Security command may result in indeterminate results, then the command shall not be deemed to have completed successfully.

1.1.11 Security mode states

See **Figure 1** and **Table 2**. When the power is off, the Security attributes are as in Table 2, but are not reportable.

Table 2 - Summary of Security States and Attributes

Security State	Security Attributes				
	Power	Enabled (ID word 85, bit 1)	Locked (ID word 128, bit 2)	Expired (ID word 128, bit 4)	Frozen (ID word 128, bit 3)
SEC0	off	0	0	0	0
SEC1	on	0	0	0	0
SEC2	on	0	0	0 or 1	1
SEC3	off	1	0	0	0
SEC4	on	1	1	0 or 1	0
SEC5	on	1	0	0 or 1	0
SEC6	on	1	0	0 or 1	1

Table 3 - Security mode command actions

Command	Disabled (SEC1)	Locked (SEC4)	Unlocked (SEC5)	Frozen (SEC2 or SEC6)
CFA ERASE SECTORS	Executable	Command aborted	Executable	Executable
CFA REQUEST EXTENDED ERROR CODE	Executable	Executable	Executable	Executable
CFA TRANSLATE SECTOR	Executable	Executable	Executable	Executable
CFA WRITE MULTIPLE WITHOUT ERASE	Executable	Command aborted	Executable	Executable
CFA WRITE SECTORS WITHOUT ERASE	Executable	Command aborted	Executable	Executable
CHECK MEDIA CARD TYPE	Executable	Command aborted	Executable	Executable
CHECK POWER MODE	Executable	Executable	Executable	Executable
CONFIGURE STREAM	Executable	Command aborted	Executable	Executable
DEVICE CONFIGURATION	Executable	Command aborted	Executable	Executable
DEVICE RESET	Executable	Executable	Executable	Executable
DOWNLOAD MICROCODE	Vendor Specific	Vendor Specific	Vendor Specific	Vendor Specific
EXECUTE DEVICE DIAGNOSTIC	Executable	Executable	Executable	Executable
FLUSH CACHE	Executable	Command aborted	Executable	Executable
FLUSH CACHE EXT	Executable	Command aborted	Executable	Executable
GET MEDIA STATUS	Executable	Command aborted	Executable	Executable
IDENTIFY DEVICE	Executable	Executable	Executable	Executable
IDENTIFY PACKET DEVICE	Executable	Executable	Executable	Executable
IDLE	Executable	Executable	Executable	Executable
IDLE IMMEDIATE	Executable	Executable	Executable	Executable
MEDIA EJECT	Executable	Command aborted	Executable	Executable
MEDIA LOCK	Executable	Command aborted	Executable	Executable
MEDIA UNLOCK	Executable	Command aborted	Executable	Executable
NOP	Executable	Executable	Executable	Executable
NV CACHE	Executable	Command aborted	Executable	Executable
PACKET	Executable	Command aborted	Executable	Executable
READ BUFFER	Executable	Executable	Executable	Executable
READ DMA	Executable	Command aborted	Executable	Executable
READ DMA EXT	Executable	Command aborted	Executable	Executable
READ DMA QUEUED	Executable	Command aborted	Executable	Executable
READ DMA QUEUED EXT	Executable	Command aborted	Executable	Executable
READ LOG EXT	Executable	Executable	Executable	Executable
READ LOG DMA EXT	Executable	Executable	Executable	Executable
READ MULTIPLE	Executable	Command aborted	Executable	Executable
READ MULTIPLE EXT	Executable	Command aborted	Executable	Executable
READ NATIVE MAX ADDRESS	Executable	Executable	Executable	Executable
READ NATIVE MAX ADDRESS EXT	Executable	Executable	Executable	Executable
READ SECTOR(S)	Executable	Command aborted	Executable	Executable
READ SECTOR(S) EXT	Executable	Command aborted	Executable	Executable
READ STREAM DMA EXT	Executable	Command aborted	Executable	Executable
READ STREAM EXT	Executable	Command aborted	Executable	Executable
READ VERIFY SECTOR(S)	Executable	Command aborted	Executable	Executable
READ VERIFY SECTOR(S) EXT	Executable	Command aborted	Executable	Executable
<u>SCT Long Segment Access</u>	<u>Executable</u>	<u>Command aborted</u>	<u>Executable</u>	<u>Executable</u>
<u>SCT Write Same</u>	<u>Executable</u>	<u>Command aborted</u>	<u>Executable</u>	<u>Executable</u>
<u>SCT Error Recovery Control</u>	<u>Executable</u>	<u>Command aborted</u>	<u>Executable</u>	<u>Executable</u>
<u>SCT Feature Control</u>	<u>Executable</u>	<u>Command aborted</u>	<u>Executable</u>	<u>Executable</u>
<u>SCT Data Tables</u>	<u>Executable</u>	<u>Command aborted</u>	<u>Executable</u>	<u>Executable</u>
<u>SCT Read Status</u>	<u>Executable</u>	<u>Executable</u>	<u>Executable</u>	<u>Executable</u>
SECURITY DISABLE PASSWORD	Executable	Command aborted	Executable	Command aborted
SECURITY ERASE PREPARE	Executable	Executable	Executable	Command aborted
SECURITY ERASE UNIT	Executable	Executable	Executable	Command aborted
SECURITY FREEZE LOCK	Executable	Command aborted	Executable	Executable
SECURITY SET PASSWORD	Executable	Command aborted	Executable	Command aborted
SECURITY UNLOCK	Command aborted	Executable	Executable	Command aborted
SERVICE	Executable	Command aborted	Executable	Executable

SET FEATURES	Executable	Executable	Executable	Executable
SET MAX ADDRESS	Executable	Command aborted	Executable	Executable
SET MAX ADDRESS EXT	Executable	Command aborted	Executable	Executable

(continued)

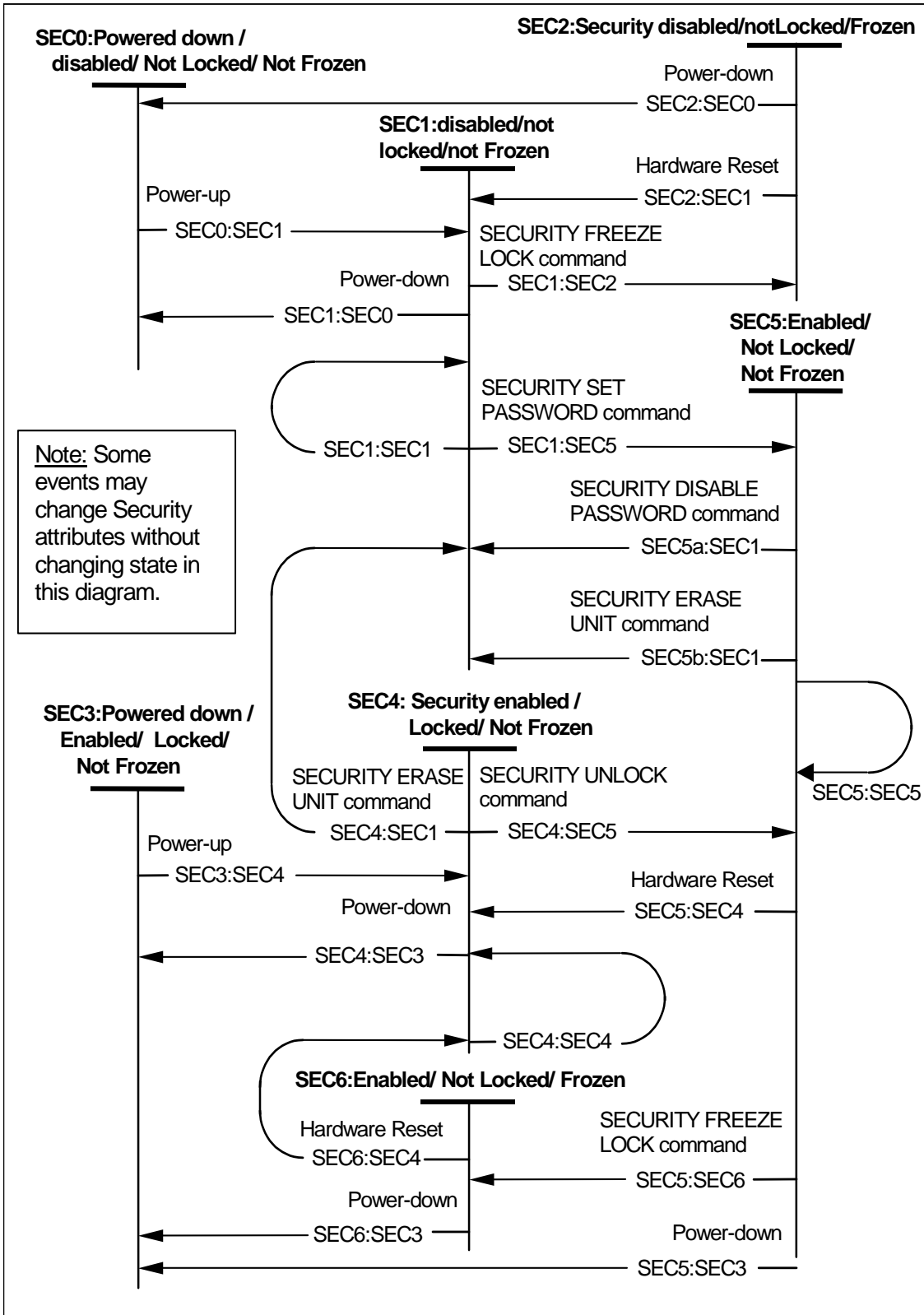
Table 3 - Security mode command actions (continued)

Command	Disabled (SEC1)	Locked (SEC4)	Unlocked (SEC5)	Frozen (SEC2 or SEC6)
SET MAX SET PASSWORD	Executable	Command aborted	Executable	Executable
SET MAX LOCK	Executable	Command aborted	Executable	Executable
SET MAX FREEZE LOCK	Executable	Command aborted	Executable	Executable
SET MAX UNLOCK	Executable	Command aborted	Executable	Executable
SET MULTIPLE MODE	Executable	Executable	Executable	Executable
SLEEP	Executable	Executable	Executable	Executable
SMART DISABLE OPERATIONS	Executable	Executable	Executable	Executable
SMART ENABLE/DISABLE AUTOSAVE	Executable	Executable	Executable	Executable
SMART ENABLE OPERATIONS	Executable	Executable	Executable	Executable
SMART EXECUTE OFF-LINE IMMEDIATE	Executable	Executable	Executable	Executable
SMART READ DATA	Executable	Executable	Executable	Executable
SMART READ LOG	Executable	Executable	Executable	Executable
SMART RETURN STATUS	Executable	Executable	Executable	Executable
SMART WRITE LOG ¹	Executable	Executable	Executable	Executable
STANDBY	Executable	Executable	Executable	Executable
STANDBY IMMEDIATE	Executable	Executable	Executable	Executable
TRUSTED RECEIVE	Executable	Command aborted	Executable	Executable
TRUSTED RECEIVE DMA	Executable	Command aborted	Executable	Executable
TRUSTED SEND	Executable	Command aborted	Executable	Executable
TRUSTED SEND DMA	Executable	Command aborted	Executable	Executable
WRITE BUFFER	Executable	Executable	Executable	Executable
WRITE DMA	Executable	Command aborted	Executable	Executable
WRITE DMA EXT	Executable	Command aborted	Executable	Executable
WRITE DMA FUA EXT	Executable	Command aborted	Executable	Executable
WRITE DMA QUEUED	Executable	Command aborted	Executable	Executable
WRITE DMA QUEUED EXT	Executable	Command aborted	Executable	Executable
WRITE DMA QUEUED FUA EXT	Executable	Command aborted	Executable	Executable
WRITE LOG EXT ¹	Executable	Executable	Executable	Executable
WRITE LOG DMA EXT ¹	Executable	Executable	Executable	Executable
WRITE MULTIPLE	Executable	Command aborted	Executable	Executable
WRITE MULTIPLE EXT	Executable	Command aborted	Executable	Executable
WRITE MULTIPLE FUA EXT	Executable	Command aborted	Executable	Executable
WRITE SECTOR(S)	Executable	Command aborted	Executable	Executable
WRITE SECTOR(S) EXT	Executable	Command aborted	Executable	Executable
WRITE STREAM DMA EXT	Executable	Command aborted	Executable	Executable
WRITE STREAM EXT	Executable	Command aborted	Executable	Executable

¹ Writing to SMART Log E0h or E1h (SCT) is prohibited when Security is Locked.

(concluded)

Figure 1 - Security State Mode Diagram



1.1.12 Details about each state and transition

State SEC0: Powered down/Security disabled: This ~~mode~~state shall be entered when the device is powered-down with the Security ~~Mode~~ feature set disabled.

Transition SEC0:SEC1: When the device is powered-up, the device shall make a transition to the SEC1: Security disabled/not Frozen state, ~~and initialize the IDENTIFY DEVICE or IDENTIFY PACKET DEVICE data.~~

State SEC1: Security disabled/not Frozen: This ~~mode~~state shall be entered when the device is powered-up or a hardware reset is received with the Security ~~Mode~~ feature set disabled or when the Security ~~Mode~~ feature set is disabled by a SECURITY DISABLE PASSWORD or SECURITY ERASE UNIT command.

In this state, the device shall respond to all commands except those indicated as Command Aborted in Table 3 “Disabled” column.

When entering this state from power-on or hardware reset, the device shall set the attempt limit to five.

~~The device shall initialize IDENTIFY DEVICE or IDENTIFY PACKET DEVICE field values in accordance with Table 4. While in this state, IDENTIFY DEVICE and IDENTIFY PACKET DEVICE shall report values as described in Table 4.~~

Table 4 - IDENTIFY settings for values reported in Security state SEC1

<u>Word</u>	<u>Bit position</u>	<u>Value</u>	<u>Description</u>
82	1	1	Security Mode feature set is supported
85	1	0	There is no active User password.
128	0	copy of word 82, bit 1	Security Mode feature set is supported
128	1	copy of word 85, bit 1	Security Mode feature set is disabled
128	2	0	device is not locked
128	3	0	device is not frozen
<u>128</u>	<u>4</u>		<u>On power-on or hardware reset, clear to zero; otherwise, do not modify this value.</u>
128	8	0	security level is not ‘maximum’

Transition SEC1:SEC0: When the device is powered-down, the device shall make a transition to the SEC0: Powered down/Security disabled state.

~~**Transition SEC1:SEC1:** When the device receives a hardware reset, the device shall make a transition to the SEC1: Security disabled/not Frozen state. [Editor's note: Only transitions which change state are shown.]~~

Transition SEC1:SEC2: When a SECURITY FREEZE LOCK command is received successful, the device shall make a transition to the SEC2: Security disabled/Frozen state.

Transition SEC1:SEC5: When a SECURITY SET (user) PASSWORD command is received successful, the device shall save the User password, update the Security Level and make a transition to the SEC5: Unlocked/not frozen state.

Transition SEC1:SEC1: When a Hardware reset occurs the device shall remain in state SEC1.

When a successful SECURITY SET (master) PASSWORD command is received, the Master password and the optional Master Password Identifier shall be saved, and the device shall remain in state SEC1. The Security Level shall remain unchanged.

State SEC2: Security disabled/Frozen: This ~~mode state~~ shall be entered when the device receives a SECURITY FREEZE LOCK command while in the SEC1:Security disabled/not Frozen state.

In this state, the device shall respond to all commands except those indicated as Command Aborted in Table 3 "Frozen" column

The device shall ~~initialize~~report the following IDENTIFY DEVICE or IDENTIFY PACKET DEVICE data when in this state:

word 128, bit 3 shall be set to one (frozen)

Transition SEC2:SEC0: When the device is powered-down, the device shall make a transition to the SEC0: Powered down/Security disabled state.

Transition SEC2:SEC1: When the device receives a hardware reset, the device shall make a transition to the SEC1: Security disabled/not Frozen state. ~~[Editor's note: Frozen state is only exited after a power-on reset. This is a bug that has persisted and was never discovered before.]~~

State SEC3: Powered down/Security enabled: This ~~mode state~~ shall be entered when the device is powered-down with the Security ~~Mode~~ feature set enabled.

Transition SEC3:SEC4: When the device is powered-up, the device shall make a transition to the SEC4: Security enabled/locked state.

State SEC4: Security enabled/Locked: This ~~mode~~state shall be entered when the device is powered-up or a hardware reset is received with the Security ~~Mode~~ feature set enabled.

In this state, the device shall respond to all commands except those indicated as Command Aborted in Table 3 “Locked” column.

When entering this state from power-on or hardware reset, the device shall set the attempt limit to five.

The device shall ~~initialize~~report IDENTIFY DEVICE or IDENTIFY PACKET DEVICE field values in accordance with Table 5 .

Table 5 - IDENTIFY settings for Security state SEC4

Word	Bit(s)	Value	Description
82	1	1	Security Mode feature set is supported
85	1	1	There is an active User password.
128	0	copy of word 82, bit 1	Security Mode feature set is supported
128	1	copy of word 85, bit 1	Security Mode feature set is enabled.
128	2	1	device is locked
128	3	0	device is not frozen
128	4		Note 1: On power-on or hardware reset, clear to zero; otherwise, do not modify this value.
128	8	0	security level is not ‘maximum’

Transition SEC4:SEC3: When the device is powered-down, the device shall make a transition to the SEC3: Powered down/Security enabled state.

Transition SEC4:SEC4: When the device receives a hardware reset, the device shall remain in state SEC4. [~~Editor’s note: Only transitions which change state are shown.~~]

When a SECURITY UNLOCK command is received with an incorrect password, the attempt limit shall be decremented by 1, and remain in state SEC4. If attempt limit reaches 0, the expire bit shall be set to 1.

Transition SEC4:SEC5: When a ~~successful~~ SECURITY UNLOCK command is received successful, the device shall make a transition to the SEC5: UNLOCKED/NOT FROZEN state.

Transition SEC4:SEC1: When a SECURITY ERASE PREPARE command is successful ~~received~~ and is followed by a successfully completing SECURITY ERASE

UNIT command, the device shall make a transition to the SEC1: SECURITY DISABLED/NOT FROZEN state.

State SEC5: Unlocked/not Frozen: This ~~mode~~state shall be entered when ~~the device receives either a SECURITY SET (user) PASSWORD command to enable the lock or a SECURITY UNLOCK command is successful.~~

In this state, the device shall respond to all commands except those indicated as Command Aborted in Table 3 “Unlocked” column. With the exception of the SECURITY commands, execution of these commands does not cause a transition from state SEC5.

The device shall ~~initialize~~report the following IDENTIFY DEVICE or IDENTIFY PACKET DEVICE data when in this state:

- | | |
|-----------------|--|
| word 128, bit 1 | shall be set to one (enabled) |
| word 128, bit 2 | shall be cleared to zero (not locked) |
| word 128, bit 8 | shall be set to one if the Security level is ‘maximum’
shall be cleared to zero if the Security level is ‘high’ |

Transition SEC5:SEC1: When a ~~valid~~ SECURITY DISABLE PASSWORD command is ~~successful~~received, the device shall make a transition to the SEC1: Security disabled/not Frozen state.

Transition SEC5:SEC6: When a SECURITY FREEZE LOCK command is ~~successful~~received, the device shall make a transition to the SEC6: Unlocked/Frozen state.

Transition SEC5:SEC3: When the device is powered-down, the device shall make a transition to the SEC3: Powered down/Security enabled state.

Transition SEC5:SEC4: When the device receives a hardware reset, the device shall make a transition to the SEC4: Security enabled/Locked state.

Transition SEC5:SEC5: When a successful SECURITY SET (master) PASSWORD command is received, the Master password and the optional Master Password Identifier shall be saved and the device shall remain in state SEC5. The Security Level shall remain unchanged.

When a SECURITY SET (user) PASSWORD command is successful, the device shall save the User password, update the Security Level and make a transition to the SEC5: Unlocked/not frozen state.

State SEC6: Unlocked/ Frozen: This ~~mode~~state shall be entered when the device receives a SECURITY FREEZE LOCK command while SEC5: UNLOCKED/NOT FROZEN: ~~Unlocked/Locked~~ state.

In this state, the device is capable of responding to all commands except those indicated as Command Aborted in Table 3_-"Frozen" column.

The device shall initialize the following IDENTIFY DEVICE or IDENTIFY PACKET DEVICE data when in this state:

word 128, bit 3 shall be set to one (frozen)

Transition SEC6:SEC4: When the device receives a hardware reset, the device shall make a transition to the SEC4: Security enabled/Locked state. ~~[Editor's note: Frozen state is only exited after a power-on reset. This is a bug that has persisted and was never discovered before.]~~

Transition SEC6:SEC3: When the device is powered-down, the device shall make a transition to the SEC3: Powered down/Security enabled state.

1.2 Master Password ~~Revision Code~~ feature Identifier feature

This is an optional enhancement to the Security Mode feature set. Support for this feature requires that the Security Mode feature set also be supported.

1.2.1 Use Case (Informative)

The intended purpose of this feature is to assist an administrator that uses several sets of Master passwords (for use in different deployments of devices). The administrator may maintain a mapping of actual Master passwords and a corresponding Identifier. When an administrator sets a Master password, the corresponding Master Password Identifier could be also set.

When the time comes to redeploy a device for which a User password had been set (and subsequently lost), the administrator needs to know which Master password is actually valid for this individual device. Since the device never reveals the Master password but does reveal the Identifier, the administrator may obtain a hint as to which Master password was previously set.

1.2.2 Requirements

The device shall maintain a 2-byte host vendor-specific data value associated with the Master Password.

The Master Password Identifier does not indicate whether a Master Password exists or is valid.

Support for this feature is reported in the IDENTIFY DEVICE or IDENTIFY PACKET DEVICE data in word 92. Valid ~~revision code~~ identifiers are 0001h through FFEh. A value of 0000h or FFFFh indicates that the ~~Master Password Revision Code~~ this feature is not supported.

If the device supports this feature,

- A. The device shall ~~associate~~ store a non-volatile ~~revision code~~ identifier field with the stored Master password. The ~~revision code~~ identifier is maintained for the benefit of the host. The device has no required use for it.
- B. Prior to first use, the initial ~~Master Password Revision Code~~ Master Password Identifier shall be set to FFEh by the manufacturer; and
- C. ~~The device shall prevent the host from setting the revision code to an unsupported value.~~

1.3 Enhanced Security Feature Set

(This section has been moved to a separate proposal.)

1.4 DEVICE CONFIGURATION SET - B1h/C3h, PIO Data Out

1.4.1.1.1 Word 7: Command/features set supported part 1

Word 7 bit 3 is cleared to zero to disable support for the Security Mode feature set if ~~the Security Mode feature set is not enabled, is disabled,~~ and has the effect of ~~clearing bit 1 to zero in word 82 and word 85 of~~ changing the IDENTIFY DEVICE or IDENTIFY PACKET DEVICE response: clear word 82 bit 1 to zero, clear word 85 bit 1 to zero, clear words 89, 90, 92 and 128 to zero. If the Security Mode feature set is enabled, then the device shall return command aborted and make no changes.

Word 7 bit 3 is set to one to allow reporting of support for the Security Mode feature set and if the device does support the feature set has the effect of changing the IDENTIFY DEVICE or IDENTIFY PACKET DEVICE response: set word 82 bit 1 to one; clear word 85 bit 1 to zero; set word 128 bit 0 to one; set word 128 bit 5 to one if the enhanced security erase feature is supported; and setting words 89, 90 and 92 to a valid value. ~~These bits shall not be cleared if the Security feature set has been enabled.~~

~~7.10.4.6.8 Word 21: Command/features set supported part 2~~

~~Bit TBD2 — 1—Reporting of support for Enhanced Security Mode feature set is allowed.~~

~~Word 21 bit TBD2 is cleared to zero to disable reporting of support for the Enhanced Security Mode feature set, and has the effect of clearing word XXX bit XXX to zero and clearing word XXXX bit XXXX to zero of the IDENTIFY DEVICE or IDENTIFY PACKET DEVICE response. If the Security Mode feature set is not supported or the Security Mode feature set is enabled, these bits shall not be cleared and the device shall return command aborted.~~

1.5 DEVICE CONFIGURATION IDENTIFY - B1h/C2h, PIO Data In

~~7.10.3.6.8 Word 21: Command/features set supported part 2~~

~~Add this to the text (and to Table 9)~~

~~Word 21 bit TBD if set to one indicates that the device is allowed to report the support of the Enhanced Security Mode feature set.~~

1.6 IDENTIFY DEVICE - ECh, PIO Data-in

1.6.1.1 Words (84:82): Features/command sets supported

If bit 1 of word 82 is set to one, the Security Mode feature set is supported.

1.6.1.2 Words (87:85): Features/command sets enabled

If bit 1 of word 85 is set to one, then ~~Security Mode feature set~~ has been enabled by setting a User password via the SECURITY SET PASSWORD command. If bit 1 of word 85 is cleared to zero, there is no valid ~~Security Mode feature set User password~~ ~~has been disabled via the SECURITY DISABLE PASSWORD command.~~ User password. If the Security Mode feature set is not supported, this bit shall be cleared to zero.

1.6.1.3 Word 89: Time required for Security erase unit completion

Word 89 specifies the estimated time required for the SECURITY ERASE UNIT command to complete its normal mode erasure. Support of this word is mandatory if the Security Mode feature set is supported. If the Security Mode feature set is not supported, this word shall be cleared to zero.

Value	Time
0	Value not specified
1-254	(Value*2) minutes
255	>508 minutes

1.6.1.4 Word 90: Time required for Enhanced security erase unit completion

Word 90 specifies the estimated time required for the ~~ENHANCED SECURITY ERASE UNIT~~ command to complete its enhanced mode erasure. Support of this word is mandatory if support of the ~~Enhanced Security Mode~~ feature set is supported. If the Security ~~Mode~~ feature set is not supported, this word shall be cleared to zero.

Value	Time
0	Value not specified
1-254	(Value*2) minutes
255	>508 minutes

1.6.1.5 Word 92: Master Password Identifier

Word 92 contains the value of the ~~Master Password Revision Code~~ Master Password Identifier set when the Master Password was last changed. ~~Valid values are 0001h through FFFFh. A value of 0000h or FFFFh indicates that the Master Password Revision~~

~~is not supported.~~ Support of this word is mandatory if the Security Mode feature set is supported. (See 1.2). If the Security Mode feature set is not supported, this word shall contain the value ~~FFFFh, 0000h or FFFFh.~~

1.6.1.6 Word 128: Security status

Support of this word is mandatory if the Security Mode feature set is supported. If the Security Mode feature set is not supported, this word shall be cleared to zero,

Bit 8 of word 128 indicates the security level. If securitymode is enabled and the security level is high, bit 8 shall be cleared to zero. If securitymode is enabled and the security level is maximum, bit 8 shall be set to one. When securitymode is disabled, bit 8 shall be cleared to zero.

Bit 5 of word 128 set to one indicates that the ~~Enhanced security erase unit feature~~ enhanced mode of the SECURITY ERASE UNIT command is supported. ~~If bit 5 is set to one, the Enhanced security erase unit feature set is supported.~~

Bit 4 of word 128 set to one indicates that the ~~security count~~ attempt limit has expired. ~~If bit 4 is set to one, the security count is expired and SECURITY UNLOCK and SECURITY ERASE UNIT are command aborted until a power on reset or hardware reset.~~

Bit 3 of word 128 set to one indicates that security is frozen. ~~If bit 3 is set to one, the security is frozen.~~

Bit 2 of word 128 set to one indicates that security is locked. ~~If bit 2 is set to one, the security is locked.~~

Bit 1 of word 128 set to one indicates that security is enabled. ~~If bit 1 is set to one, the security is enabled.~~ This is a copy of word 85, bit 1.

Bit 0 of word 128 set to one indicates that the Security Mode feature set supported. ~~If bit 0 is set to one, security is supported.~~ This is a copy of word 82, bit 1.

1.6.1.7 Word TBD1: (additional supported bits)

Bit TBD2 — 1 = Enhanced Security feature set is supported

~~1.6.1.8~~ ~~Word TBD3: (additional enabled bits)~~

~~Bit TBD4 — 1=Enhanced Security feature set is enabled~~

1.7 IDENTIFY PACKET DEVICE - A1h, PIO Data-in

1.7.1.1 Words (84:82): Features/command sets supported

Words (84:82) shall have the content described for words (84:82) of the IDENTIFY DEVICE command except that bit 4 of word 82 shall be set to one to indicate that the PACKET Command feature set is supported.

1.7.1.2 Words (87:85): Features/command sets enabled

Words (87:85) shall have the content described for words (87:85) of the IDENTIFY DEVICE command except that bit 4 of word 85 shall be set to one to indicate that the PACKET Command feature set is supported.

1.7.1.3 Word 89: Time required for Security erase unit completion

Word 89 shall have the content described for word 89 of the IDENTIFY DEVICE command.

1.7.1.4 Word 90: Time required for Enhanced security erase unit completion

Word 90 shall have the content described for word 90 of the IDENTIFY DEVICE command.

1.7.1.5 Word (92:91): Reserved

Word 92 shall have the content described for word 92 of the IDENTIFY DEVICE command.

[Editors note: Add Words 89, 90, 92 to ID Packet Device table]

1.7.1.6 Word 128: Security status

Word 128 shall have the content described for word 128 of the IDENTIFY DEVICE command. Support of this word is mandatory if the Security ~~feature~~ Security Mode feature set is supported.

~~1.7.1.7 Word TBD1: (additional supported bits)~~

~~Bit TBD2 — 1=Enhanced Security feature set is supported~~

~~1.7.1.8 Word TBD3: (additional enabled bits)~~

~~Bit TBD4 — 1=Enhanced Security feature set is enabled~~

1.8 SECURITY DISABLE PASSWORD - F6h, PIO data-out

1.8.1 Feature Set

This command is mandatory for devices that implement the Security Mode feature set.

1.8.2 Description

The SECURITY DISABLE PASSWORD command transfers 512 bytes of data from the host. Table 6 defines the content of this information. If the password selected by word 0 matches the password previously saved by the device, the device shall disable the ~~Lock mode~~User password, and return the drive to the SEC1 state. This command shall not change the Master password. ~~The Master password shall be reactivated when a User password is set(See 1.2).~~

If the Security Level is High, either a valid Master or User password is required.

If the Security Level is Maximum, a valid User password is required. If a Master password (even if valid) is supplied, the device shall return command aborted.

This command shall only complete successfully if the Device is in Unlocked mode.

Upon successful completion, these fields of IDENTIFY DEVICE or IDENTIFY PACKET DEVICE shall be updated:

word 85, bit 1	shall be cleared to zero (no active user password)
word 128, bit 1	shall be cleared to zero (no active user password)
word 128, bit 8	shall be cleared to zero (security level is not maximum)

1.8.3 Inputs

Word	Name	Description
00h	Feature	N/A
01h	Count	N/A
02h-04h	LBA	N/A
05h	Command	F6h

1.8.4 Normal outputs

See [Table 62]

1.8.5 Error outputs

The device shall return command aborted if the command is not supported, the device is in Locked mode, or the device is in Frozen mode. The device may return error status if an Interface CRC error has occurred. See [Table 76].

1.8.6 Output Data Structure

Table 6 - Security password content

Word	Content
0	Control word
	Bit 0 Identifier 0=compare User password 1=compare Master password
	Bit Reserved (15:1)
1-16	Password (32 bytes)
17-255	Reserved

1.9 SECURITY ERASE PREPARE - F3h, Non-data

1.9.1 Feature Set

This command is mandatory for devices that implement the Security Mode feature set.

1.9.2 Description

The SECURITY ERASE PREPARE command shall be issued immediately before the SECURITY ERASE UNIT command to enable device erasing and unlocking. This command prevents accidental loss of data on the device.

1.9.3 Inputs

Word	Name	Description
00h	Feature	N/A
01h	Count	N/A
02h-04h	LBA	N/A
05h	Command	F3h

1.9.4 Normal outputs

See [Table 62]

1.9.5 Error outputs

Abort shall be set to one if the device is in Frozen mode. See [Table 76]

1.10 SECURITY ERASE UNIT - F4h, PIO data-out

1.10.1 Feature Set

This command is mandatory for devices that implement the Security Mode feature set.

1.10.2 Description

This command transfers 512 bytes of data from the host. Table 7 defines the content of this information. If the password does not match the password previously saved by the device, the device shall ~~reject the command with~~ return command aborted.

The SECURITY ERASE PREPARE command shall be completed immediately prior to the SECURITY ERASE UNIT command. If the device receives a SECURITY ERASE UNIT command without an immediately prior SECURITY ERASE PREPARE command, the device shall return command aborted for the SECURITY ERASE UNIT command.

If the attempt limit counter has already decremented to zero, then the device shall return command aborted even if a correct password has been supplied.

If the the Security mode is Disabled (e.g. there is no active user password), a valid Master password is required.

If Security is enabled, SECURITY ERASE UNIT ignores the Security Level attribute when comparing passwords, and shall accept a valid Master or User password.
~~If the Security Level is High or Maximum, either a valid Master or User password is required.~~

When Normal Erase mode is specified, the SECURITY ERASE UNIT command shall write binary zeroes to all user data areas (as determined by READ NATIVE MAX or READ NATIVE MAX EXT). IDENTIFY DEVICE or IDENTIFY PACKET DEVICE word 89 gives an estimate of the time required to complete the erasure.

The Enhanced Erase mode is optional. IDENTIFY DEVICE or IDENTIFY PACKET DEVICE word 128, bit 5 indicates whether it is supported. When Enhanced Erase mode is specified, the device shall write predetermined data patterns to all user data areas. In Enhanced Erase mode, all previously written user data shall be overwritten, including sectors that are no longer in use due to reallocation. IDENTIFY DEVICE or IDENTIFY PACKET DEVICE word 90 gives an estimate of the time required to complete the erasure.

On successful completion, ~~this command shall disable the device Lock mode~~ Security (e.g. returns the device to Security state SEC1), and ~~deactivate~~ invalidate any existing User password. ~~., however, the Masterpassword shall still be stored internally within the device and may be reactivated later when a new User password is set.~~ Any previously valid Master password remains valid and active.

~~This command shall be immediately preceded by a SECURITY ERASE PREPARE command.~~

1.11 SECURITY FREEZE LOCK - F5h, Non-data

1.11.1 Feature Set

This command is mandatory for devices that implement Security Mode feature set.

1.11.2 Description

The SECURITY FREEZE LOCK command shall set the device to Frozen mode. After command completion any other commands that update the device Lock mode shall be command aborted. Frozen mode shall be disabled by power-off or hardware reset. If SECURITY FREEZE LOCK shall be issued when the device is in Frozen mode, the command executes and the device shall remain in Frozen mode.

See [Table 3](#) for a list of commands disabled by SECURITY FREEZE LOCK.

~~Commands disabled by SECURITY FREEZE LOCK are:~~

- ~~SECURITY SET PASSWORD~~
- ~~SECURITY UNLOCK~~
- ~~SECURITY DISABLE PASSWORD~~
- ~~SECURITY ERASE PREPARE~~
- ~~SECURITY ERASE UNIT~~

Upon successful completion, these fields of IDENTIFY DEVICE or IDENTIFY PACKET DEVICE shall be updated:

word 128, bit 3 shall be set to one (frozen)

1.11.3 Inputs

Word	Name	Description
00h	Feature	N/A
01h	Count	N/A
02h-04h	LBA	N/A
05h	Command	F5h

1.11.4 Normal outputs

See [Table 62].

1.11.5 Error outputs

Abort shall be set to one if the device is in Frozen mode. See [Table 76].

1.12 SECURITY SET PASSWORD - F1h, PIO data-out

1.12.1 Feature Set

This command is mandatory for devices that implement the Security Mode feature set.

1.12.2 Description

This command transfers 512 bytes of data from the host. Table 9 defines the content of this information. The data transferred controls the function of this command. Table 8 defines the interaction of the identifier and security level bits.

1.12.2.1 Setting the Master Password

If a master password is specified, the device shall save the supplied master password in a non-volatile location. The Security Level shall remain unchanged. -No changes shall be made to IDENTIFY DEVICE or IDENTIFY PACKET DEVICE words 85 or 128.

~~In addition, if the device supports the Master Password Revision Code~~Master Password Identifier feature and a valid ~~revision code~~identifier is supplied (see 1.2), the device shall save the ~~revision code~~identifier in a non-volatile location. This new value shall be returned, and return it in word 92 of IDENTIFY DEVICE or IDENTIFY PACKET DEVICE result data. If the host attempts to set the identifier to a invalid value (0000h or FFFFh), the device shall preserve the existing identifier and return command aborted.

If the device does not support the ~~Master Password Revision Code~~Master Password Identifier feature, the device shall not ~~change word 92~~validate the identifier field, and shall not change word 92 of IDENTIFY DEVICE or IDENTIFY PACKET DEVICE.

~~The revision code field shall be returned in the IDENTIFY DEVICE data word 92. The valid revision codes are 0001h through FFFEh. A value of 0000h or FFFFh indicates that the Master Password Revision Code is not supported.~~

1.12.2.2 Setting the User Password

If a user password is specified, the device shall save the User password in a non-volatile location and, update the Security Level. The Master password identifier shall not be changed. These and these fields of IDENTIFY DEVICE or IDENTIFY PACKET DEVICE shall be updated:

word 85, bit 1	shall be set to one (Security enabled)
word 128, bit 1	shall be set to one (Security enabled)
word 128, bit 8	shall indicate the Security Level

Table 8 - Identifier and security level bit interaction

Identifier	Level	Command result
User	High	The password supplied with the command shall be saved as the new User password. The Lock mode Security shall be enabled from the next power-on or hardware reset. The device shall <u>can</u> be unlocked by either the User password or the Master password. <u>The Security Level shall be updated.</u>
User	Maximum	The password supplied with the command shall be saved as the new User password. Security The Lock mode shall be enabled from the next power-on or hardware reset. The device shall <u>can</u> be unlocked by only the User password. The Master password is still stored in the device but shall not be used to unlock the device. <u>The Security Level shall be updated.</u>
Master	High or Maximum <u>Ignored</u>	This combination shall set a Master password but shall not enable or disable the Lock mode Security. The Security Level is not changed. Master password revision code <u>The Master Password Identifier shall be set to the value in Master Password Revision Code</u> Master Password Identifier field (if supported).

1.12.3 Inputs

Word	Name	Description
00h	Feature	N/A
01h	Count	N/A
02h-04h	LBA	N/A
05h	Command	F1h

1.12.3.1 Input data structure

Table 9 – SECURITY SET PASSWORD data content

<u>Word</u>	<u>Content</u>
<u>0</u>	<u>Control word</u>
<u>Bit 0</u>	<u>Identifier</u> <u>0=set User password</u> <u>1=set Master password</u>
<u>Bits (7:1)</u>	<u>Reserved</u>
<u>Bit 8</u>	<u>Security Level</u> <u>0=High</u> <u>1=Maximum</u>
<u>Bit (15:9)</u>	<u>Reserved</u>
<u>1-16</u>	<u>Password (32 bytes)</u>
<u>17</u>	<u>Master Password Identifier (valid if word 0, bit 0 = 1, and if the device supports the Master Password Identifier feature)</u>
<u>18-255</u>	<u>Reserved</u>

1.12.4 Normal outputs

See [Table 62]

1.12.5 Error outputs

Abort shall be set to one if the device is Locked or in Frozen mode. The device may return error status if an Interface CRC error has occurred. See [Table 76].

See-

Table – Identifier and security level bit interaction

Identifier	Level	Command result
User	High	The password supplied with the command shall be saved as the new User password. The Lock mode shall be enabled from the next power-on or hardware reset. The device shall then be unlocked by either the User password or the previously set Master password.
User	Maximum	The password supplied with the command shall be saved as the new User password. The Lock mode shall be enabled from the next power-on or hardware reset. The device shall then be unlocked by only the User password. The Master password previously set is still stored in the device but shall not be used to unlock the device.
Master	High or Maximum	This combination shall set a Master password but shall not enable or disable the Lock mode. The security level is not changed. Master password revision code Master Password Identifier set to the value in Master Password Revision Code Master Password Identifier field.

1.13 SECURITY UNLOCK - F2h, PIO data-out

1.13.1 Feature Set

This command is mandatory for devices that implement the Security Mode feature set.

1.13.2 Description

This command transfers 512 bytes of data from the host. Table 6 defines the content of this information.

If the Identifier bit is set to Master and the device is in high security level, then the password supplied shall be compared with the stored Master password. If the device is in maximum security level then the ~~unlock shall be rejected~~ device shall return command aborted.

If the Identifier bit is set to user then the device shall compare the supplied password with the stored User password. This shall occur even if the Security is already Unlocked.

If the Security Level is High, either a valid Master or User password is required.

If the Security Level is Maximum, a valid User password is required. If a Master password (even if valid) is supplied, the device shall return command aborted.

If the ~~unlock~~ attempt limit counter has already decremented to zero, then the device shall return command aborted even if a correct password has been supplied.

If the password compare fails then the device shall return command aborted to the host and decrements the ~~unlock~~ attempt limit counter. ~~This counter shall be initially set to five and shall be decremented for each password mismatch when SECURITY UNLOCK is issued and the device is locked.~~ When this counter reaches zero, IDENTIFY DEVICE or IDENTIFY PACKET DEVICE word 128 bit 4 shall be set to one, and SECURITY UNLOCK and SECURITY ERASE UNIT commands shall be return command aborted until a power-on reset or a hardware reset. SECURITY UNLOCK commands issued when the device is unlocked have no effect on the unlock counter.

Upon successful completion IDENTIFY DEVICE or IDENTIFY PACKET DEVICE shall be updated:

word 128, bit 2 shall be cleared to zero (not locked)

1.13.3 Inputs

Word	Name	Description
00h	Feature	N/A
01h	Count	N/A
02h-04h	LBA	N/A
05h	Command	F2h

1.13.4 Normal outputs

See [Table 62]

1.13.5 Error outputs

If the device is in Frozen mode or an invalid password is supplied or the attempt limit has expired, the device shall return command aborted.

~~Abort shall be set to one if the device is in Frozen mode.~~ The device may return error status if an Interface CRC error has occurred. See [Table 76]. |