

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: October 24, 2006

Revision History:

- 0: Initial revision
- 1: Incorporate feedback from Dec. 2005 plenary. Split the Enhancements to a separate proposal.
- 2: Incorporate feedback from March 14, 2006 ad hoc meeting.
- 3: Incorporate feedback from March 28, 2006 ad hoc meeting.
- 4: Incorporate feedback from Plenary #58 (April 2006), and ad hoc meetings (May 17, 2006 and May 24, 2006)
- 5: Incorporate feedback from ad hoc meetings: June 7 and 14, 2006 .
6. List feedback from Plenary #59 (June 21, 2006)
7. Incorporate feedback from Plenary #60 (August 2006)
8. Change the state diagram to a Visio format

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.

Open Issues

- 1) Shall hardware reset be removed as an exit from Frozen states ?
 - a. Resolution:
 - i. No. fix the one text reference (in the feature description) that is bad. The figure is correct.
Create an informative note (where the text is being corrected) saying that the host 'should' reissue a SECURITY FREEZE LOCK after hardware reset.

- 2) May SECURITY ERASE UNIT and SECURITY DISABLE PASSWORD be allowed to decrement the attempt counter for failed password comparisons ? If so, from which states may this be allowed ?
- a. Resolution:
- Since ATA7 is silent on the issue: remain silent on the issue. ~~In this clarifications proposal, remove the 'may'. No changes to the spec on this issue e.g. The SECURITY UNLOCK command is the only command that decrements the counter.~~
 - Consider any new restrictions in a future 'security enhancements' proposal
Move this change to the future 'security enhancements' proposal.
- 3) May SECURITY ERASE UNIT and SECURITY DISABLE PASSWORD be allowed to reset the attempt counter on entry to state SEC1 ?
- a. Resolution:
- Since ATA7 is silent on the issue: remain silent on the issue.
 - Consider any new restrictions ~~This is not a clarification: consider this in a future the 'security enhancements' proposal~~
The counter is only cleared on power-on or hardware reset.
- 4) In Table 4, the DCO command has been split into separate subcommands. Are the suggested table values correct ?
- a. Resolution:
- Keep DCO subcommands as ~~separate~~ a single row in the table marked as 'executable'.
 - But do not make DCO SET and DCO RESTORE aborted when Security is Frozen. ~~Move this change~~ Consider any new restrictions to a future the 'security enhancements' proposal. ~~Keep them as executable here.~~
- 5) In table 4, WRITE LOG EXT has been changed from 'command aborted' to 'executable' in order to be symmetric with SMART WRITE LOG. Is this acceptable ?
- a. Resolution:
- This ~~is~~ would be an enhancement, not a clarification: ~~Keep it as 'command aborted'.~~
 - Consider any changes in a future 'security enhancements' proposal.
- 6) Does a successful SECURITY UNLOCK command reset the attempt counter (and clear the PasswordAttemptCounterExceeded flag) ?
- a. Resolution:
- Since ATA7 is silent on the issue: remain silent on the issue.
 - Consider any new restrictions in a future 'security enhancements' proposal. ~~This is an enhancement, not a clarification.~~

- 7) New text has been proposed for DCO RESTORE and DCO SET. Are these acceptable ?
- a. Resolution:
 - i. Dco restore: Acceptable: see editors note in dco restore
 - ii. Dco set: acceptable. See editors note in dco set
- 8) From state SEC1: If a SECURITY ERASE UNIT or a SECURITY DISABLE PASSWORD command is received (with a Master password), ‘shall’ the device compare the password ? or ‘may’ the device ignore the password ? Is this a clarification or an enhancement ?
- a. Resolution:
 - ~~SECURITY ERASE UNIT specifically says the password SHALL be compared (regardless of state).~~
 - i. Make sure that e05162r0 (approved) is integrated with this clarifications document.
 - ii. Since ATA7 is silent on the issue: remain silent on the issue.
 - iii. Consider any new restrictions in a future ‘security enhancements’ proposal. Consider Ignoring the password is the be moved to the ‘security enhancements’ proposal.
- 9) In the text following the state diagram, shall each reference to each state name ALSO have the tags “enabled/locked/frozen”, etc. that is appropriate to each state ?
- a. Resolution: do not keep all the tags with each reference
- 10) Incorporate the Visio version of the state diagram
- a. Resolution:

Proposal

I propose that the following ~~text~~ be incorporated into ATA8-ACS as a full replacement for the referenced sections.

These terms are to be added to the Glossary

<u>Security Is 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. IDENTIFY DEVICE reports that the Security feature set is ‘not supported’.</u>
<u>Security Is Disabled</u>	<u>The Security 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 feature set. The terms ‘Security Is Locked’ and ‘Security Is Unlocked’ are not applicable. (e.g. Security states SEC0, SEC1, SEC2).</u>
<u>Security Is Enabled</u>	<u>The Security feature set is supported, and a valid User password has been set. (e.g. Security states SEC3, SEC4, SEC5, SEC6).</u>
<u>Security Is Locked</u>	<u>Security is enabled. In addition, access to the device is restricted. (e.g. Security state SEC4).</u>
<u>Security Is Unlocked</u>	<u>Security is enabled. A SECURITY UNLOCK command was successful, allowing access to the device. (e.g. Security state SEC5, SEC6).</u>
<u>Security Is Frozen</u>	<u>Security may be either enabled or disabled. Changes to Security states are not allowed until after the next power-on or hardware reset. (e.g. Security states SEC2, SEC6).</u>
<u>Security Is Not Frozen</u>	<u>Security may be either enabled or disabled. Changes to Security states are allowed (e.g. Security states SEC1, SEC4, SEC5).</u>
<u>Master Password Capability</u>	<u>The Master Password Capability indicates whether or not the Master password may be used to unlock the device. This was formerly know as ‘Security Level’.</u>
<u>Security Level</u>	<u>See Master Password Capability .</u>
<u>Password Attempt Counter Exceeded</u>	<u>There were too many attempts to unlock the device with an incorrect password. Further unlock attempts are denied until a power-on or hardware reset. This is a name associated with IDENTIFY DEVICE, word 128, bit 4.</u>

1.1 Security **Mode** feature set

1.1.1 Overview

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~~
- ~~—Locked: True or False~~
- ~~—Security Level: High or Maximum~~
- ~~—Attempt Limit counter~~
- ~~—Frozen: True or False~~
- ~~—User password~~
- ~~—Master password~~
- ~~—~~

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

1.1.2 ~~Master and User Passwords~~

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

1.1.2.1.1 User Password

The User password is used to create a lock to block execution of some commands, including preventing access to all user data on the device. The User password may be used to unlock the device to allow access.

~~The Ssecurity system is enabled by sending a user setting a User password to the device with the SECURITY SET PASSWORD command. When ~~the Ssecurity system is Enabled,~~ the device is automatically Locked (i.e., access to user data on the device is denied) after a power-cycle-on reset is processed until the User password is sent to the device with the a SECURITY UNLOCK command completes successfully.~~

1.1.2.1.2 Master Password

The Master password is a password that may be used to unlock the device if the User password is lost or if an administrator requires access (e.g. to repurpose a device).

~~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 device may contain both a valid Master and a valid User password. 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 (i.e., does not Lock the device after the next power-on reset has been processed).~~

~~1.1.3 High and Maximum Security Level~~ Master Password Capability

~~A device with Security enabled has two ways of using the Master password. This capability has values of '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 Master Password Capability is set to High, either the User or Master password may be used interchangably. the device requires the SECURITY UNLOCK command and the Master password to unlock. See Table 1.~~

~~When the security level Master Password Capability 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 a valid 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.~~

Table 1 - Interaction of [Master Password Capability](#) and Passwords ([when Security is not frozen](#))

Security Enabled	Master Password Capability	Passwords Defined	Password Supplied	Actions Taken by Security Commands		
				SECURITY DISABLE PASSWORD	SECURITY UNLOCK	Properly Prefaced SECURITY ERASE UNIT
No	Disabled / N/A	master only	master (correct)	N	N	E
No	N/A disabled	master only	user (not valid)	A	A	A
Yes	High	master and user	master (correct)	E	E	E
Yes	High	master and user	user (correct)	E	E	E
Yes	Maximum	master and user	master (correct)	A	A	E
Yes	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 [attribute states](#) until a following [power cycle](#) [power-on reset](#) or [hardware reset](#). The purpose of the SECURITY FREEZE LOCK command is to prevent password setting attacks on the security system.

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 [\(requires a password\)](#)
- SECURITY ERASE PREPARE
- SECURITY ERASE UNIT [\(requires a password\)](#)
- SECURITY FREEZE LOCK
- SECURITY DISABLE PASSWORD [\(requires a password\)](#)

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.~~

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 FFFEH 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 Master Password Capability value when comparing passwords, and shall accept either 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 Master Password Capability~~ 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 Master Password Capability~~ was set to Maximum during the last SECURITY SET (~~user~~) PASSWORD command, the device shall ~~not unlock~~ return command aborted ~~for SECURITY UNLOCK or SECURITY DISABLE PASSWORD~~ 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 Password Attempt Limit Counter for SECURITY UNLOCK command

The device shall have an ~~attemptpassword attempt-limit~~ counter. The purpose of this counter is to defeat repeated trial attacks. The counter shall be decremented while in state SEC4, whenever the SECURITY UNLOCK command fails because of an invalid After each failed User or Master password SECURITY UNLOCK command, the counter is decremented.

~~SECURITY ERASE UNIT and SECURITY DISABLE PASSWORD commands may decrement the counter for failed password comparisons~~ editors note: from which states ?

Once the counter reaches zero, it shall not be decremented, and ~~When the counter value reaches zero~~ the ~~EXPIRE PasswordAttemptCounterExceeded~~ bit ((bit 4) of IDENTIFY DEVICE (data word 128, bit 4) ~~is~~ shall be set to one, and the SECURITY UNLOCK and SECURITY ~~UNIT ERASE ERASE UNIT~~ commands ~~are~~ shall be command aborted until after processing the next the device is powered off power-on or hardware reset.

The ~~EXPIRE PasswordAttemptCounterExceeded~~ bit shall be cleared to zero after by processing either a power-on or a hardware reset.
~~None of the commands in the Security feature set shall clear this bit.~~

The counter shall ~~be~~ set to five (5) after a power-on or hardware reset. None of the commands in the Security feature set shall re-initialize this counter.

1.1.10 Resets

~~When Software Reset and Device Reset occurs between commands, the device shall not change any Security attribute of the device. When a 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 Security is disabled or enabled.~~

~~Any reset or power-down event that occurs during the execution of a Security command may result in indeterminate results.~~

1.1.11.1.10 Security mode states

See [Figure 1](#) and [Table 2](#). When the power is off, the Security characteristics are as in [Table 2](#), but are not reportable.

Table 2 - Summary of Security States and AttributeCharacteristics

Security State	Security <u>AttributeCharacteristics</u>				
	Power	Enabled (ID word 85, bit 1)	Locked (ID word 128, bit 2)	Frozen (ID word 128, bit 3)	Expired Password Attempts Exceeded (ID word 128, bit 4)
SEC0	off	0	<u>N/A</u> 0	<u>N/A</u>	<u>N/A</u> 0
SEC1	on	0	0	<u>0</u>	0
SEC2	on	0	0	<u>1</u>	<u>varies 0-∞</u> ‡
SEC3	off	1	<u>0</u> N/A	<u>N/A</u>	<u>N/A</u> 0
SEC4	on	1	1	<u>0</u>	<u>0-∞</u> ‡ <u>varies</u>
SEC5	on	1	0	<u>0</u>	<u>varies 0-∞</u> ‡
SEC6	on	1	0	<u>1</u>	<u>varies 0-∞</u> ‡

Table 3—Security mode command actions

Table 4 - Security mode command actions [Editors note: collapse this table: SEC1 and SEC5 columns allow all cmds with DOWNLOAD MICROCODE being the only exception - one normative statement will suffice.]

Command	Disabled (SEC1) [Editors note: this entire column is new]	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	Command aborted 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
SCT Long Segment Access	Executable	Command aborted	Executable	Executable
SCT Write Same	Executable	Command aborted	Executable	Executable
SCT Error Recovery Control	Executable	Command aborted	Executable	Executable
SCT Feature Control	Executable	Command aborted	Executable	Executable
SCT Data Tables	Executable	Command aborted	Executable	Executable
SCT Read Status	Executable	Executable	Executable	Executable
SECURITY DISABLE PASSWORD	Executable	Command aborted	Executable	Command aborted

Table 4 - Security mode command actions [Editors note: collapse this table: SEC1 and SEC5 columns allow all cmds with DOWNLOAD MICROCODE being the only exception - one normative statement will suffice.]

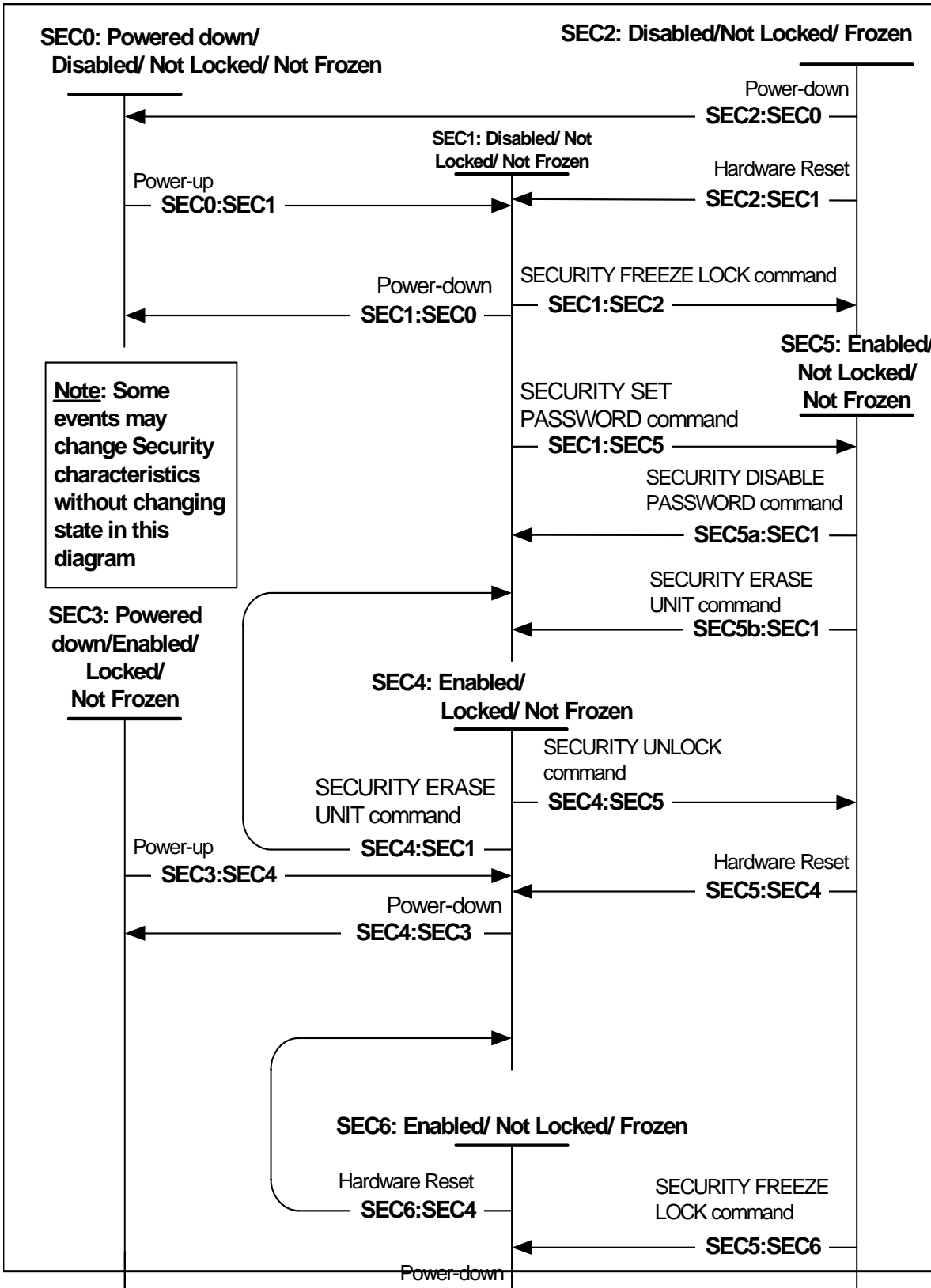
Command	Disabled (SEC1) [Editors note: this entire column is new]	Locked (SEC4)	Unlocked (SEC5)	Frozen (SEC2 or SEC6)
SECURITY ERASE PREPARE	Executable	Executable	Executable	Command aborted
SECURITY ERASE UNIT	Executable	Executable	Executable	Command aborted
SECURITY FREEZE LOCK	Executable	Command aborted	Executable	Executable
SECURITY SET PASSWORD	Executable	Command aborted	Executable	Command aborted
SECURITY UNLOCK	Command aborted Executable	Executable	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
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	Command aborted Executable [Editors note: in ATA7 this was 'aborted'. This proposal would change this to Executable because SMART WRITE LOG is 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

Table 4 - Security mode command actions [Editors note: collapse this table: SEC1 and SEC5 columns allow all cmds with DOWNLOAD MICROCODE being the only exception - one normative statement will suffice.]

Command	Disabled (SEC1) [Editors note: this entire column is new]	Locked (SEC4)	Unlocked (SEC5)	Frozen (SEC2 or SEC6)
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. SET MAX ADDRESS EXT Executable Command aborted Executable Executable				

|

Figure 1 - Security State **Mode** Diagram





1.1.421.1.11 Details about each state and transition

State SEC0: Powered down/Security Disabled/Not Locked/ Not Frozen: 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 ~~state~~the SEC1: ~~Security disabled/not Frozen state, and initialize the IDENTIFY DEVICE or IDENTIFY PACKET DEVICE data.~~

State SEC1: Security Disabled/Not Locked/ 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.

~~When entering this state from~~after processing a power-on or hardware reset, the device shall initialize the password attempt counter and clear the PasswordAttemptCounterExceeded flag

~~In this state, the device shall respond to all commands except those indicated as Command Aborted in “Disabled” column.~~In this state, the device shall respond to all commands as specified in the “Disabled” column of ~~Table 4~~Table 4. With the exception of the SECURITY commands, execution of these commands shall not cause a transition from state SEC1.

~~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~~In this state, IDENTIFY DEVICE and IDENTIFY PACKET DEVICE shall report values as described in ~~Table 5~~Table 5.

Table ~~554~~ - IDENTIFY- ~~settings for~~settings for 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>Varies</u>	<u>PasswordAttemptCounterExceeded</u>

			<u>1= counter exceeded</u> <u>0= counter not exceeded</u>
128	8	0	<u>security level Master Password Capability is not 'maximum'</u>

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

~~[Editors note: change state names to include the full text?]~~

Transition SEC1:SEC1:

When a SECURITY SET (master) PASSWORD command completes successfully, the Master password and the optional Master Password Identifier shall be saved, and the device shall remain in state SEC1. The Master Password Capability shall remain unchanged.

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

Transition SEC1:SEC5: When a SECURITY SET (user) PASSWORD command ~~is completes received~~ successfully, the device shall save the User password, update the Master Password Capability and make a transition to state the SEC5: Unlocked/not frozen state.

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

In this state, the device shall respond to all commands as specified in the "Frozen" column of Table 4. Execution of any of these commands shall not cause a transition from state SEC2.

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

The device shall report IDENTIFY DEVICE or IDENTIFY PACKET DEVICE field values in accordance with Table 6.

Table 6 - IDENTIFY settings for Security state SEC2

<u>Word</u>	<u>Bit(s)</u>	<u>Value</u>	<u>Desription</u>
<u>82</u>	<u>1</u>	<u>1</u>	<u>Security feature set is supported</u>
<u>85</u>	<u>1</u>	<u>0</u>	<u>There is not an active User password.</u>

<u>128</u>	<u>0</u>	<u>copy of word 82, bit 1</u>	<u>Security feature set is supported</u>
<u>128</u>	<u>1</u>	<u>copy of word 85, bit 1</u>	<u>Security feature set is not enabled.</u>
<u>128</u>	<u>2</u>	<u>0</u>	<u>device is not locked</u>
<u>128</u>	<u>3</u>	<u>1</u>	<u>device is frozen</u>
<u>128</u>	<u>4</u>	<u>varies</u>	<u>PasswordAttemptCounterExceeded</u> <u>1= counter exceeded</u> <u>0= counter not exceeded</u>
<u>128</u>	<u>8</u>	<u>varies</u>	<u>Master Password Capability</u> <u>0=high/User password disabled</u>

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

Transition SEC2:SEC1: When the device receives a hardware reset, the device shall make a transition to ~~state~~ SEC1: ~~Security disabled/not Frozen state~~.

State SEC3: Powered down/Security Enabled/ Locked/ Not Frozen: 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 ~~state~~ the SEC4: ~~Security enabled/locked state~~.

State SEC4: Security Enabled/ Locked/ 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 enabled.

In this state, the device shall respond to all commands as specified in the “Locked” column of ~~Table 4~~Table 4. With the exception of the SECURITY commands, execution of these commands shall not cause a transition from state SEC4.

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

When entering this state from power-on or hardware reset, the device shall ~~set initialize the attempt password attempt limit counter to five and clear the PasswordAttemptCounterExceeded flag.~~

The device shall ~~initialize report~~ IDENTIFY DEVICE or IDENTIFY PACKET DEVICE field values in accordance with ~~Table 7~~ Table 7.

Table 75 - 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	<u>varies</u>	<u>PasswordAttemptCounterExceeded</u> <u>1= counter exceeded</u> <u>0= counter not exceeded</u> <u>Note 1: On power-on or hardware reset, clear to zero; otherwise, do not modify this value.</u>
128	8	<u>0 varies</u>	<u>security level</u> <u>Master Password Capability is not ‘maximum’</u> <u>0=high</u> <u>1=maximum</u>

Transition SEC4:SEC1: When a SECURITY ERASE UNIT command completed successfully, the device shall make a transition to state SEC1.

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

Transition SEC4:SEC4: ~~When the device receives a hardware reset, the device shall state. [Editor’s note: Only transitions which change state are shown.]~~ When a SECURITY UNLOCK command is received with an incorrect password, the password attempt counter shall be decremented by 1, and remain in state SEC4.

If password attempt counter reaches 0, the PasswordAttemptCounterExceeded bit (IDENTIFY DEVICE word 128, bit 4) shall be set to 1.

After execution of the SECURITY ERASE PREPARE command, the device remains in state SEC4.

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

[editors note: does the counter get re-initialized on a successful UNLOCK ? or does the counter retain its value ? Current text says only on poweron or hardware reset.]

~~**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: Security Enabled/ Not Locked/ Not Frozen~~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 as specified in the “Unlocked” column of ~~Table 4~~Table 4. With the exception of the SECURITY commands, execution of these commands shall not cause a transition from state SEC5.

~~In this state, the device shall respond to all commands except those indicated as Command Aborted in “Unlocked” column~~

~~The device shall report IDENTIFY DEVICE or IDENTIFY PACKET DEVICE field values in accordance with [Table 8](#)~~

~~The device shall initialize 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’~~

Table 8 - IDENTIFY settings for Security state SEC5

<u>Word</u>	<u>Bit(s)</u>	<u>Value</u>	<u>Description</u>
<u>82</u>	<u>1</u>	<u>1</u>	<u>Security feature set is supported</u>
<u>85</u>	<u>1</u>	<u>1</u>	<u>There is an active User password.</u>
<u>128</u>	<u>0</u>	<u>copy of word 82, bit 1</u>	<u>Security feature set is supported</u>
<u>128</u>	<u>1</u>	<u>copy of word 85, bit 1</u>	<u>Security feature set is enabled.</u>
<u>128</u>	<u>2</u>	<u>0</u>	<u>device is not locked</u>
<u>128</u>	<u>3</u>	<u>0</u>	<u>device is not frozen</u>
<u>128</u>	<u>4</u>	<u>varies</u>	<u>PasswordAttemptCounterExceeded</u> <u>1= counter exceeded</u> <u>0= counter not exceeded</u>
<u>128</u>	<u>8</u>	<u>varies</u>	<u>Master Password Capability</u> <u>0=high</u> <u>1=maximum</u>

Transition SEC5:SEC1: When a ~~valid~~ SECURITY DISABLE PASSWORD ~~or a SECURITY ERASE UNIT~~ 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 ~~state the~~ SEC3: ~~Powered down/Security enabled~~ state.

Transition SEC5:SEC4: When the device receives a hardware reset, the device shall make a transition to ~~state 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, the Master Password Capability shall remain unchanged, and the device shall remain in state SEC5..

When a SECURITY SET (user) PASSWORD command is successful, the device shall save the User password, update the Master Password Capability and shall remain in state SEC5.

After execution of the SECURITY ERASE PREPARE command, the device remains in state SEC4.

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

State SEC6: Security Enabled/ Not Locked/ Frozen~~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 shall respond to all commands as specified in the “Frozen” column of ~~Table 4~~Table 4. With the exception of the SECURITY commands, execution of these commands shall not cause a transition from state SEC6.

~~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 report IDENTIFY DEVICE or IDENTIFY PACKET DEVICE field values in accordance with ~~Table 9~~ Table 9.

Table 9 - IDENTIFY settings for Security state SEC6

<u>Word</u>	<u>Bit(s)</u>	<u>Value</u>	<u>Description</u>
<u>82</u>	<u>1</u>	<u>1</u>	<u>Security feature set is supported</u>
<u>85</u>	<u>1</u>	<u>1</u>	<u>There is an active User password.</u>
<u>128</u>	<u>0</u>	<u>copy of word 82, bit 1</u>	<u>Security feature set is supported</u>
<u>128</u>	<u>1</u>	<u>copy of word 85, bit 1</u>	<u>Security feature set is enabled.</u>
<u>128</u>	<u>2</u>	<u>0</u>	<u>device is not locked</u>
<u>128</u>	<u>3</u>	<u>1</u>	<u>device is frozen</u>
<u>128</u>	<u>4</u>	<u>varies</u>	<u>PasswordAttemptCounterExceeded</u> <u>1= counter exceeded</u> <u>0= counter not exceeded</u>
<u>128</u>	<u>8</u>	<u>varies</u>	<u>Master Password Capability</u> <u>0=high</u> <u>1=maximum</u>

~~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 state 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 state 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, which is a prerequisite. 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 FFFEh. 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 ~~value is not modified by the device~~ 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 FFFEh by the manufacturer.

1.3 DEVICE CONFIGURATION SET RESTORE - B1h/C03h, PIO Data Out/Non-data

[Editors note: this following text is new]

If Security is Enabled prior to receiving this DCO RESTORE command, and the DCO RESTORE would unsupport the Security feature set, then the device shall return command aborted and make no changes;

1.3.1.1.1 Word 7: Command/features set supported part 1

If DCO RESTORE changes reporting of support for the Word 7 bit 3 is cleared to zero to disable support for the Security feature set from 'allowed' to 'not allowed', then any stored Master Password and optional Master Password Identifier shall be preserved. if the Security Mode feature set is not enabled, 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 commands shall respond as follows: 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.

If DCO RESTORE changes reporting of support for the Security feature set from 'not allowed' to 'allowed', and if DCO IDENTIFY would indicate that reporting of that support is 'allowed', then Word 7 bit 3 is set to one to allow reporting of support for the Security Mode feature set and if the device shall set the Security state to SEC1, setting IDENTIFY DEVICE data to the values described in Table 5, and shall restore the saved Master password and Master Password Identifier ; otherwise, the Security state shall not change. [editors note: explicitly state IDENTIFY DEVICE word/bit values, restore the preserved (attempt count, expire bit, master pswd, master pswd identifier, etc.)]

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.

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

1.4.1.1.1 Word 7: Command/features set supported part 1

ATA7 says:

Word 7 bit 3 is cleared to zero to disable support for the Security feature set and has the effect of clearing bit 1 to zero in word 82 and word 85 of the IDENTIFY DEVICE or IDENTIFY PACKET DEVICE response. These bits shall not be cleared if the Security feature set has been enabled.

Replace that with this text:

Word 7 bit 3 is cleared to zero: If Security is Enabled, then the device shall return command aborted. ~~If DCO SET would change reporting of support for the Security feature set from 'allowed' to 'not allowed',~~ If Security is Disabled then any stored Master Password and Master Password Identifier ~~[editors note: shall be preserved.~~ ~~and IDENTIFY DEVICE or IDENTIFY PACKET DEVICE~~ commands shall respond as follows: clear word 82 bit 1 to zero, clear word 85 bit 1 to zero, clear words 89, 90, 92 and 128 to zero.

Word 7 bit 3 is set to one: ~~If DCO SET does not change reporting of support for the Security feature set from 'not allowed' to 'allowed', and if DCO IDENTIFY would indicate that reporting of that support is 'allowed', then the device shall set the Security state to SEC1; otherwise, The Security state shall not change.~~

|

1.4 IDENTIFY DEVICE - ECh, PIO Data-in

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

If bit 1 of word 82 is set to one, the Security [Mode](#) feature set is supported.

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

If bit 1 of word 85 is set to one, the [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.

1.4.1.31.4.1.4 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

1.4.1.41.4.1.5 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

1.4.1.51.4.1.6 Word 92: Master Password [Revision Code Identifier](#)

[If either the Security feature set or the Master Password Identifier feature are not supported, word 92 shall contain the value 0000h or FFFFh](#)

If the Security feature set and the Master Password Identifier feature are supported, 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 contains the value FFFFh.

1.4.1.61.4.1.7 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 levelMaster Password Capability. If security**mode** is enabled and the security levelMaster Password Capability is high, bit 8 shall be cleared to zero. If security**mode** is enabled and the security levelMaster Password Capability is maximum, bit 8 shall be set to one. When security**mode** is disabled, bit 8 shall be cleared to zero.

Bit 5 of word 128 set to one indicates that the Enhanced security erase unit featureenhanced 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 countattemptpassword attempt limitcounter has expireddecremented to zero. This is also known as the “PasswordAttemptCounterExceeded” bit. 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 is supported. If bit 0 is set to one, security is supported. This is a copy of word 82, bit 1.

1.5 IDENTIFY PACKET DEVICE - A1h, PIO Data-in

1.5.1.1 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.

1.5.1.2 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.

1.5.1.3 Word 89: Time required for Security erase unit completion

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

1.5.1.4 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.

1.5.1.5 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]

1.5.1.6 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.

1.6 SECURITY DISABLE PASSWORD - F6h, PIO data-out

1.6.1 Feature Set

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

1.6.2 Description

The SECURITY DISABLE PASSWORD command transfers 512 bytes of data from the host. ~~Table 10~~Table 10 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 or the Master Password Identifier. ~~The Master password shall be reactivated when a User password is set(See 1.2).~~

This command shall return command aborted if the Security feature set is not supported, if Security is Locked (SEC4) or is Frozen (states SEC2 or SEC6).

When Security is Disabled: ~~Editors note: is this an enhancement or clarification?~~ If and the Identifier bit is set to User, then the device shall return command aborted.

When Security is Enabled, and the Master Password Capability is 'High':

- a. If the Identifier bit is set to Master, then the password supplied shall be compared with the stored Master password.
- b. If the Identifier bit is set to User, then the password supplied shall be compared with the stored User password.

When Security is Enabled, and the Master Password Capability is 'Maximum'

- a. If the Identifier bit is set to Master, then the device shall return command aborted, even if the supplied Master password is valid.
- b. If the Identifier bit is set to User, then the password supplied shall be compared with the stored User password.

~~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 <u>U</u> ser password)
word 128, bit 1	<u>is a copy of word 85, bit 1</u>

word 128, bit 8 shall be cleared to zero ([security level Master Password Capability](#) is not [Mmaximum](#))

1.6.3 Inputs

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

1.6.4 Normal outputs

See [Table 62]

1.6.5 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].

1.6.6 Output Data Structure [\(Sent by the Host\)](#)

Table ~~10196~~ [— Security password content SECURITY DISABLE PASSWORD data](#)

Word	Content									
0	Control word <table border="1"> <thead> <tr> <th>Bit</th> <th>Field Name</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Bit 0</td> <td>Identifier</td> <td>0=compare User password 1=compare Master password</td> </tr> <tr> <td>Bit (15:1)</td> <td>Reserved</td> <td></td> </tr> </tbody> </table>	Bit	Field Name	Description	Bit 0	Identifier	0=compare User password 1=compare Master password	Bit (15:1)	Reserved	
Bit	Field Name	Description								
Bit 0	Identifier	0=compare User password 1=compare Master password								
Bit (15:1)	Reserved									
1-16	Password (32 bytes)									
17-255	Reserved									

1.7 SECURITY ERASE PREPARE - F3h, Non-data

1.7.1 Feature Set

This command is mandatory for devices that implement the Security [Mode](#) feature set.

1.7.2 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.~~

1.7.3 Inputs

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

1.7.4 Normal outputs

See [Table 62]

1.7.5 Error outputs

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

1.8 SECURITY ERASE UNIT - F4h, 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

This command transfers 512 bytes of data from the host. [Table 11](#) 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 ~~and the previous command was not without an immediately prior a successful~~ SECURITY ERASE PREPARE command, the device shall return command aborted for the SECURITY ERASE UNIT command.

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

When Security is Disabled and If the Identifier bit is set to User, then the device shall return command aborted.

When Security is Enabled, and the Master Password Capability is 'High':

- a. If the Identifier bit is set to Master, then the password supplied shall be compared with the stored Master password.
- b. If the Identifier bit is set to User, then the password supplied shall be compared with the stored User password.

When Security is Enabled, and the Master Password Capability is 'Maximum':

- a. If the Identifier bit is set to Master, then the password supplied shall be compared with the stored Master password.
- c. If the Identifier bit is set to User, then the password supplied shall be compared with the stored User password.

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

~~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, ~~t~~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 and Master Password Identifier remains valid and active.~~

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

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 Master Password

Capability

is not Mmaximum)

1.8.3 Inputs

Word	Name	Description
00h	Feature	N/A
01h	Count	N/A
02h-04h	LBA	N/A
05h	Command	F4h

1.8.4 Normal outputs

See [Table 62]

1.8.5 Error outputs

~~Abort shall be set to one~~The device shall return command aborted if the ~~device is in Frozen mode~~, not immediately preceded by a SECURITY ERASE PREPARE command, or if Enhanced mode was requested but the device does not support it, or of an invalid password was specified, or if the data area is not successfully overwritten. The device may return error status if an Interface CRC error has occurred. See [Table 76].

1.8.6 Output Data Structure [\(Sent by the Host\)](#)Table ~~1147~~ - SECURITY ERASE UNIT [passworddata](#)

Word	Content		
0	Control word		
	<u>Bit</u>	<u>Field Name</u>	<u>Description</u>
	Bit 0	Identifier	0=Compare User password 1=Compare Master password
	1	Erase mode	0=Normal Erase mode 1=Enhanced Erase mode
	Bit (15:2)	Reserved	
1-16	Password (32 bytes)		
17-255	Reserved		

1.9 SECURITY FREEZE LOCK - F5h, Non-data

1.9.1 Feature Set

This command is mandatory for devices that implement Security [Mode](#) feature set.

1.9.2 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~~ is issued when the device is in Frozen mode, the command executes and the device shall remain in Frozen mode.

See [Table 4](#) 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)

1.9.3 Inputs

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

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 SET PASSWORD - F1h, 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 12](#) defines the content of this information. ~~The data transferred controls the function of this command. defines the interaction of the identifier and security level bits. The command sets only one password at a time.~~

1.10.2.1 Setting the Master Password

If a ~~M~~master password is specified, the device shall save the supplied ~~M~~master password in a non-volatile location. ~~The Master Password Capability shall remain unchanged. This does not cause any changes 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 Master Password Identifier identifier from a valid to an invalid value (0000h or FFFFh), the device shall preserve the existing identifier~~Master Password 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.~~ This shall not be cause to return command aborted.

~~1.10.2.2 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.~~Setting the User Password

If a ~~U~~user password is specified, the device shall save the ~~U~~user password in a non-volatile location ~~and, update the Security Level~~Master Password Capability. ~~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)
<u>word 128, bit 8</u>	<u>shall indicate the Security Level</u> Master Password Capability

1.12.31.10.3 Inputs

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

1.10.3.1 Output data structure (Sent by the Host)**Table 12 – SECURITY SET PASSWORD data**

<u>Word</u>	<u>Content</u>															
<u>0</u>	<u>Control word</u>															
	<table border="1"> <thead> <tr> <th><u>Bit</u></th> <th><u>Field Name</u></th> <th><u>Description</u></th> </tr> </thead> <tbody> <tr> <td><u>0</u></td> <td><u>Identifier</u></td> <td><u>0=set User password</u> <u>1=set Master password</u></td> </tr> <tr> <td><u>(7:1)</u></td> <td><u>Reserved</u></td> <td></td> </tr> <tr> <td><u>8</u></td> <td><u>Security Level Master Password Capability</u></td> <td><u>0=High</u> <u>1=Maximum</u></td> </tr> <tr> <td><u>(15:9)</u></td> <td><u>Reserved</u></td> <td></td> </tr> </tbody> </table>	<u>Bit</u>	<u>Field Name</u>	<u>Description</u>	<u>0</u>	<u>Identifier</u>	<u>0=set User password</u> <u>1=set Master password</u>	<u>(7:1)</u>	<u>Reserved</u>		<u>8</u>	<u>Security Level Master Password Capability</u>	<u>0=High</u> <u>1=Maximum</u>	<u>(15:9)</u>	<u>Reserved</u>	
<u>Bit</u>	<u>Field Name</u>	<u>Description</u>														
<u>0</u>	<u>Identifier</u>	<u>0=set User password</u> <u>1=set Master password</u>														
<u>(7:1)</u>	<u>Reserved</u>															
<u>8</u>	<u>Security Level Master Password Capability</u>	<u>0=High</u> <u>1=Maximum</u>														
<u>(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>															

Table 8 – Identifier and Security Level Master Password Capability bit Interaction**1.10.4 Normal outputs**

See [Table 62]

1.10.5 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].

1.11 SECURITY UNLOCK - F2h, PIO data-out

1.11.1 Feature Set

This command is mandatory for devices that implement the Security [Mode](#) feature set.

1.11.2 Description

This command transfers 512 bytes of data from the host. [Table 14](#) defines the content of this information.

[When Security is Disabled and if the Identifier bit is set to User, then the device shall return command aborted.](#)

[When Security is Enabled, and the Master Password Capability is 'High':](#)

- [c. If the Identifier bit is set to Master, then the password supplied shall be compared with the stored Master password.](#)
- [d. If the Identifier bit is set to User, then the password supplied shall be compared with the stored User password.](#)

[When Security is Enabled, and the Master Password Capability is 'Maximum'](#)

- [b. If the Identifier bit is set to Master, then the device shall return command aborted.](#)
- [d. If the Identifier bit is set to User, then the password supplied shall be compared with the stored User password.](#)

~~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.~~

~~If the password attempt 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~~password 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, this field of IDENTIFY DEVICE or IDENTIFY PACKET DEVICE shall be updated:

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

1.11.3 Inputs

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

1.11.4 Normal outputs

See [Table 62]

1.11.5 Error outputs

If the device is in Frozen mode or an invalid password is supplied or the ~~attempt~~password attempt limitcounter has ~~expired~~decremented to zero, 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].

1.11.6 Output Data Structure (Sent by the Host)

Table 14 – SECURITY UNLOCK data

<u>Word</u>	<u>Content</u>									
<u>0</u>	<u>Control word</u> <table border="1"> <thead> <tr> <th><u>Bit</u></th> <th><u>Field Name</u></th> <th><u>Description</u></th> </tr> </thead> <tbody> <tr> <td><u>0</u></td> <td><u>Identifier</u></td> <td><u>0=compare User password</u> <u>1=compare Master password</u></td> </tr> <tr> <td><u>(15:1)</u></td> <td><u>Reserved</u></td> <td></td> </tr> </tbody> </table>	<u>Bit</u>	<u>Field Name</u>	<u>Description</u>	<u>0</u>	<u>Identifier</u>	<u>0=compare User password</u> <u>1=compare Master password</u>	<u>(15:1)</u>	<u>Reserved</u>	
<u>Bit</u>	<u>Field Name</u>	<u>Description</u>								
<u>0</u>	<u>Identifier</u>	<u>0=compare User password</u> <u>1=compare Master password</u>								
<u>(15:1)</u>	<u>Reserved</u>									
<u>1-16</u>	<u>Password (32 bytes)</u>									
<u>17-255</u>	<u>Reserved</u>									