Proposal for adding Secure Mode to ATA Specification

30 March 1994

Pete McLean
Maxtor Corporation
2190 Miller Drive
Longmont, Colorado 80501
(303) 678-2149

1.0 Background

With the introduction of small, removable hard-disk drives, particularly PCMCIA drives, users now have a convenient, removable data storage medium. This medium provides relatively high data capacity in a size and weight that conveniently fits in one's shirt pocket. This medium is easily transportable from one host to another. Users are now free to travel taking their data with them, creating or updating it on mobile systems or systems other than their own.

This new freedom comes with a problem. When the media containing users valuable data is not removable from their system, the system's security protection prevents access by others. With a small removable medium, the user's data is now subject to loss or theft.

This specification describes a method for limiting access to data stored on small form factor, removable hard disk drives to only authorized users or host systems. To accomplish this, a drive is placed in "secure mode" by a user. Having done so, whenever the drive is placed in a host, it must be "unlocked" before it will execute data transfer commands. "Unlocking" is accomplished by providing the drive with a valid "password".

2.0 Operational Overview

Whether a drive supports secure mode and, if so, the secure mode state can be determined by issuing an ATA command (SECURE_STATE).

The drive may be set into either Secure Mode Read Only where the drive may be read but not written, or Secure Mode Read/Write where no data transfers can be executed.

The drive is set into "secure mode" by an ATA command (SET_SECURE_RO or SET_SECURE_RW). The user may set up to four "passwords" each up to 512 bytes in length and the host system will create an "emergency password". The user may also specify that one or more of the "passwords" must be matched to "unlock" the drive. The number of matches required to unlock the drive is placed in the Features register before issuing the SET_SECURE_XX command. The SET_SECURE_XX command resembles a write command in that the sector count is valid and the command includes the transfer of n sectors of data to the drive. Each of the n sectors represents a unique "password". If the user defined password contains fewer than 512 bytes, the password will be zero filled to complete a full sector, so that a password sent when the drive is installed on one system will be exactly the same as a password sent when installed on another system.

When in "secure mode" and "locked", non-data transfer commands will be executed normally, however, all data transfer commands, i.e., commands that read or modify user data on the disk, will be rejected with error if in secure mode RW and write commands, i.e., commands that modify user data on the disk, will be rejected if in secure mode RO. When "unlocked", all commands will execute normally.

An ATA command will allow the drive to be taken out of "secure mode" (DISABLE_SECURE), If in "secure mode" and "unlocked", a drive will accept the DISABLE_SECURE command and go out of "secure mode" and delete all passwords. If the drive is in "secure mode" and has not been "unlocked", it will reject the command with errors set.

When inserted/powered up, the drive will go through the standard PCMCIA startup and ATA startup and the state of "secure mode" will be noted. If in "Secure Mode RW" and "locked", the drive will respond to non-data transfer commands but will reject transfer commands until an UNLOCK command is received. If in "Secure Mode RO" and "locked, the drive will reject all write commands until an UNLOCK command is received. The UNLOCK command is another ATA command and again resembles a write command. It must have sector count set at the number of sector matches required to unlock the drive and will include the transfer of one sector of data to the memory card for each required match. When data is

received, it will not be written, instead it will be compared to the valid "passwords" stored. If the required matches are found, the drive will "unlock" and function normally. If no match is found, errors will be reported in response to the command and the drive will remain "locked". An unlock command with only one password, the emergency password will always unlock the drive.

When the drive is unlocked, a flag tells the drive when to relock. It may be set such that the drive will automatically lock when powered down or it may require a LOCK command to lock the drive. The flag to disable locking at power down is provided for systems that frequently remove power from the drive. The passwords remain valid, and normal secure mode locking at power down can be re-enabled by issuing another UNLOCK command.

When the UNLOCK command is issued and the drive is already in the unlocked state, the command is executed and if the match count and passwords are not valid, i.e., the command would not have unlocked the drive an error is returned. Thus when in unlocked state, passwords can be verified using the UNLOCK command. The flag for locking the drive at power down must be valid when verifying passwords.

The LOCK command locks the drive immediately on receipt.

The ADD_PASSWORDS, REMOVE_PASSWORDS, and MODIFY_MATCH commands allow the user to modify the set of passwords and number of matches required to unlock the drive.

3.0 Secure Mode Commands

The following ATA commands are used in the implementation of Secure Mode. The Secure Mode state of the drive resulting from the execution of these commands must be maintained by the drive when powered-down. This state includes whether or not the drive is in secure mode, if it is locked, the number of password matches required to unlock and the existing set of valid passwords.

Class	Command	Command Code	Parameters Used				
			FR	SC	SN	CY	DH
1	SECURE_STATE	EAh	y		80	y	D
3	SET_SECURE_RW	EBh	y	y	81	y	D
3	SET_SECURE_RO	EBh	y	y	82	y	D
3	ADD_PASSWORDS	EBh	y	y	83	y	D
3	REMOVE_PASSWORDS	EBh	y	y	84	y	D
1	MODIFY_MATCH	EAh	y		85	y	D
1	DISABLE_SECURE	EAh			86	y	D
3	UNLOCK	EBh	y	y	87	y	D
1	LOCK	EAh			88	y	D

The host will set the Cylinder High Register with the ASCII character S (53h) and the Cylinder Low Register with the ASCII character M (4Dh) prior to command assertion. The drive will validate these contents before executing the command and will invert the contents of the Cylinder Registers. All secure mode commands Abort if the cylinder registers do not contain these values. Thus upon completion of the command, the host will know that the drive supports secure mode even if the command fails due to an error.

3.1 SECURE_STATE Command

This command allows the host to determine the current secure mode state of the drive. It will be accepted and executed at any time. Flow of this command is shown in figure 1.

Upon completion of this command, the contents of the drive registers will be as follows:

Cylinder High - ACh
Cylinder Low - B2h
Features - Version number of secure mode implemented by the drive
Sector count -

7	6	5	4	3	2	1	0
Secure State			LockFlag	0	Match Count		

Bits7:6 - Secure State
Bit 7 - Secure Set R/W- If set indicates the drive has been set in Secure Mode Read/Write.
Bit 6 - Secure Set RO - If set indicates the drive has been set in Secure Mode Read Only.
Bit 5 - Unlocked - If set indicates the drive has been Unlocked so that data transfer commands will be executed.
Bit 4 - Lock Flag - this bit is only valid if the Secure State is 011 or 101.
0 - indicates drive will assume the Locked State when powered down
1 - indicates drive can only be locked by issuing the LOCK command
Bit 3 - Zero
Bit 2:0 - Number of password matches required to unlock drive

Valid Secure State (bits 7:5) are:

000 Indicates the drive is not in secure mode

100 Indicates the drive is set into Secure mode R/W, but is locked. Data transfer commands, i.e., commands that read or modify user data on the disk, will be rejected.

010 Indicates the drive is set into Secure mode RO, but is locked. Write data transfer commands, i.e., commands that modify user data on the disk, will be rejected.

101 Indicates the drive is set into Secure Mode R/W, and is unlocked. All data transfer commands will execute.

011 Indicates the drive is set into Secure Mode RO, and is unlocked. All data transfer commands will execute.

3.2 SET_SECURE_RW Command

This command is used to set a drive into Secure Mode Read/Write, define the valid set of passwords and the number of password matches required to unlock a drive. Flow of this command is shown in figure 2.

If the drive is not in Secure Mode when the command is received, the value set in the Features register indicates the number of matches that will be required to unlock the drive. The value set in the Sector Count register indicates the number of 512 byte passwords that will be passed with this command including the Emergency password. If either the Features register low order four bits or the Sector Count register contain a value less than 1 or greater than 5, the command is not executed and Abort error is returned. If the number in the Features register low order four bits is greater than the number in the Sector Count register, the command is not executed and Abort error is returned.

Use of the Emergency password is optional. If the most significant bit of the Features register is set, the first password received by the drive is considered to be the Emergency password. The number of matches required and the passwords received with the command become the valid passwords and match count

values. Upon successful completion of this command, the secure state will reflect Secure Mode RW set, unlocked, value 101. The contents of the Cylinder Registers will be ACh and B2h.

The Emergency password shall be created by the host by asking the user a series of questions. This password will consist of 18 twenty byte fields. Each field will contain the ASCII response to one question. If the user response is longer than twenty bytes, the field will contain the first twenty bytes of the response (i.e., response will be truncated). If the response is less than twenty bytes the end of the field will be zero filled. The last 152 bytes of the password will be zero filled. The Emergency password may only be modified by removing the drive from secure mode, then setting into secure mode again. The questions in order will be:

Question	Field	Password bytes
Last Name?	0	0-19
First Name?	1	20-39
Home address - street?	2	40-59
Home address - city?	3	60-79
Home address - state?	4	80-99
Home Address - country?	5	100-119
Home phone number?	6	120-139
Employer's name?	7	140-159
Work address - street?	8	160-179
Work address - city?	9	180-199
Work address - state?	10	200-219
Work address - country?	11	220-239
Work phone number?	12	240-259
Place of birth - city?	13	260-279
Place of birth - state?	14	280-299
Place of birth - country?	15	300-319
Date of birth?	16	320-339
Mother's maiden name?	17	340-359
Zero fill		360-511

If the drive is in Secure Mode when this command is received, the command will not be executed and an Abort error is returned.

3.3 SET_SECURE_RO Command

This command is used to set a drive into Secure Mode Read Only, define the valid set of passwords and the number of password matches required to unlock a drive. Flow of this command is shown in figure 2.

If the drive is not in Secure Mode when the command is received, the value set in the Features register indicates the number of matches that will be required to unlock the drive. The value set in the Sector Count register indicates the number of 512 byte passwords that will be passed with this command including the Emergency password. If either the Features register low order four bits or the Sector Count register contain a value less than 1 or greater than 5, the command is not executed and Abort error is returned. If the number in the Features register low order four bits is greater than the number in the Sector Count register, the command is not executed and Abort error is returned.

Use of the Emergency password is optional. If the most significant bit of the Features register is set, the first password received by the drive is considered to be the Emergency password. The number of matches required and the passwords received with the command become the valid passwords and match count values. Upon successful completion of this command, the secure state will reflect Secure Mode RO set, unlocked, value 011. The contents of the Cylinder Registers will be ACh and B2h.

The Emergency password shall be created by the host by asking the user a series of questions. This password will consist of 18 twenty byte fields. Each field will contain the ASCII response to one question. If the user response is longer than twenty bytes, the field will contain the first twenty bytes of the response (i.e., response will be truncated). If the response is less than twenty bytes the end of the field will be zero filled. The last 152 bytes of the password will be zero filled. The Emergency password may only be modified by removing the drive from secure mode, then setting into secure mode again. The questions in order will be as defined in the table shown in the SET_SECURE_RW command.

If the drive is in Secure Mode when this command is received, the command will not be executed and an Abort error is returned.

3.4 ADD_PASSWORDS Command

When the drive is in Secure Mode XX, unlocked, state 101 or 011, with an existing match count and set of valid passwords, this command is used to add passwords to the existing set of valid passwords and reset the match count. Flow of this command is shown in figure 4.

The value in the Features register will become the new match count value. The value in the Sector Count register indicates the number of passwords to be added. If the value in the Sector Count register is zero, or if the value in the Sector Count register plus the existing number of valid passwords is greater than 5, the command will be rejected and an Abort error returned. If the value in the Features register is less than 1 or greater than the value in the Sector Count register plus the number of existing valid passwords, the command will be rejected and an Abort error returned.

Upon successful completion of this command, the passwords received with this command will be added to the set of existing passwords, the match count value will be the new match count value, and the drive will be in Secure Mode XX, unlocked state, 101 or 011.

If this command is received when not in Secure Mode XX, unlocked state, 101 or 011, the command will be rejected and an Abort error returned.

3.5 REMOVE_PASSWORDS Command

When the drive is in Secure Mode XX, unlocked, state 101 or 011, with an existing match count and set of valid passwords, this command is used to remove passwords from the existing set of valid passwords and reset the match count. Flow of this command is shown in figure 5.

The value in the Features register will become the new match count value. The value in the Sector Count register indicates the number of passwords to be removed. If the existing number of valid passwords minus the value in the Sector Count register is less than 1, the command will be rejected and an Abort error returned. If the value in the Features register is less than 1 or greater than the number of existing valid passwords minus the value in the Sector Count register, the command will be rejected and an Abort error returned. The emergency password may not be removed and the command will be rejected with an Abort error if this is attempted.

Upon successful completion of this command, the passwords received with this command will be compared with the set of existing passwords and each that matches with a different password will be removed from the valid set of passwords. Passwords that do not match any valid passwords do not affect

the set of valid passwords. The match count value will be the new match count value, and the drive will be in Secure Mode XX, unlocked state, 101 or 011.

If this command is received when not in Secure Mode XX, unlocked state, 101 or 011, the command will be rejected and an Abort error returned.

3.6 MODIFY_MATCH Command

When the drive is in Secure Mode XX, unlocked, state 101 or 011, with an existing match count and set of valid passwords, this command is used to reset only the match count. Flow of this command is shown in figure 6.

The value in the Features register will become the new match count value. If the value in the Features register is less than 1 or greater than the number of existing valid passwords, the command will be rejected and an Abort error returned.

Upon successful completion of this command, the match count value will be the new match count value, and the drive will be in Secure Mode XX, unlocked state, 101 or 011.

If this command is received when not in Secure Mode XX, unlocked state, 101 or 011, the command will be rejected and an Abort error returned.

3.7 DISABLE_SECURE Command

When the drive is in Secure Mode XX, unlocked, state 101 or 011, with an existing match count and set of valid passwords, this command is used to remove the drive from Secure Mode. Flow of this command is shown in figure 7.

Upon successful completion of this command, the drive will be in state 000, not in Secure Mode. All passwords are deleted.

If this command is received when not in Secure Mode XX, unlocked state, 101 or 011, the command will be rejected and an Abort error returned.

3.8 UNLOCK Command

This command unlocks a drive in the Secure Mode, locked state to allow data transfers. Flow of this command is shown in figure 8.

If the user has forgotten the user defined passwords, the host may recreate the emergency password by asking the questions described in the SET_SECURE_XX command.

If the sector count register contains the value 1 and the password received is the emergency password the command will execute and the drive will unlock. Otherwise, the sector count register will contain the number of 512 byte passwords to be passed to the drive and matched. If this number is not equal to the number of matches specified when the drive was placed in Secure Mode, the command will be rejected and the Abort error returned.

The drive will match the password(s) received with this command with the existing set of valid passwords. If each unlock password matches with a different password in the established set of passwords, the drive will unlock.

For example, if the number of matches is specified as one and the set of passwords consists of four passwords, the single password received with the UNLOCK command will be compared to each of the four possibilities until a match is found.

If the number of matches is specified as two and the set of passwords consists of three passwords, the first password received with the UNLOCK command will be compared to each of the three possibilities until a match is found, and then the second password received with the UNLOCK command will be compared to the remaining two possibilities until a match is found.

If the UNLOCK was successful, the Features register indicates the required action to relock the drive. If the Features register contains the value 00h, the drive will assume the lock state when powered-down. If the Features register contains the value FFh, the drive will only assume the locked state when the LOCK command is received, that is, the drive may be powered-down and back up without assuming the locked state. Passwords remain valid.

If the value in the Features register is other than 00h or FFh, or if the required number of passwords received with the command do not match existing valid passwords, the command is rejected, an Abort error is returned, and the drive will remain in secure mode XX set, locked state, secure state 100 or 010. If eight UNLOCK commands are rejected with error, the drive will cease response to any command until powered-down and re powered-up.

If this command is received when the drive is in Secure Mode XX, unlocked state, 101 or 011, the command will be executed and if the match count or passwords do not match, an Abort error will be returned but the drive will remain unlocked. Thus when in the unlocked state, this command can be used to verify match count and passwords. The Features register is used as described above to set or clear the Lock Flag.

Upon successful completion, the secure state will reflect 101 or 011, Secure Mode XX set and unlocked. Having been unlocked, the drive will now accept and execute all data transfer commands.

If this command is received when not in Secure Mode , state 000, the command will be rejected and an Abort error returned.

3.9 LOCK Command

This command will lock a drive any time the drive is in secure mode XX, unlocked, state 101 or 011. If the drive was unlocked with the Features register value FFh, this is the only means of locking the drive. If the drive was unlocked with the Features register value 00h, either this command or powering-down the drive will cause the drive to assume the locked state. Flow of this command is shown in figure 9.

Upon successful completion of this command the drive will be in secure mode XX, locked, state 100 or 010.

If this command is received when the drive is not in Secure Mode, state 000, or in Secure Mode XX, locked, state 100 or 010, the command will be rejected and an Abort error returned.

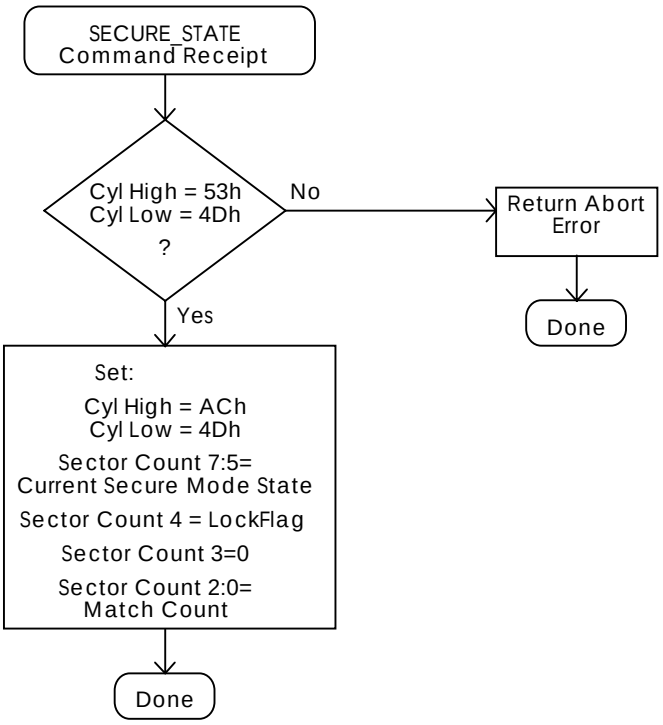

Figure 1 - SECURE_STATE Command Execution

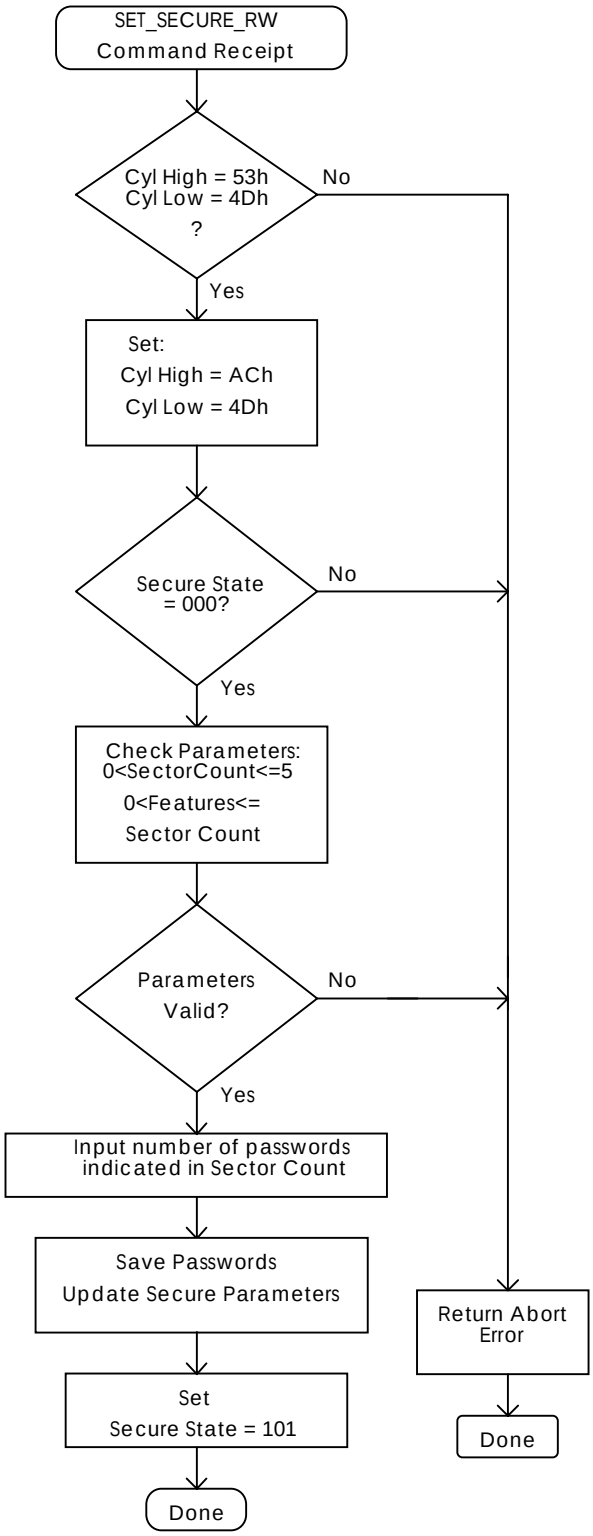

Figure 2 - SET_SECURE_RW Command Execution

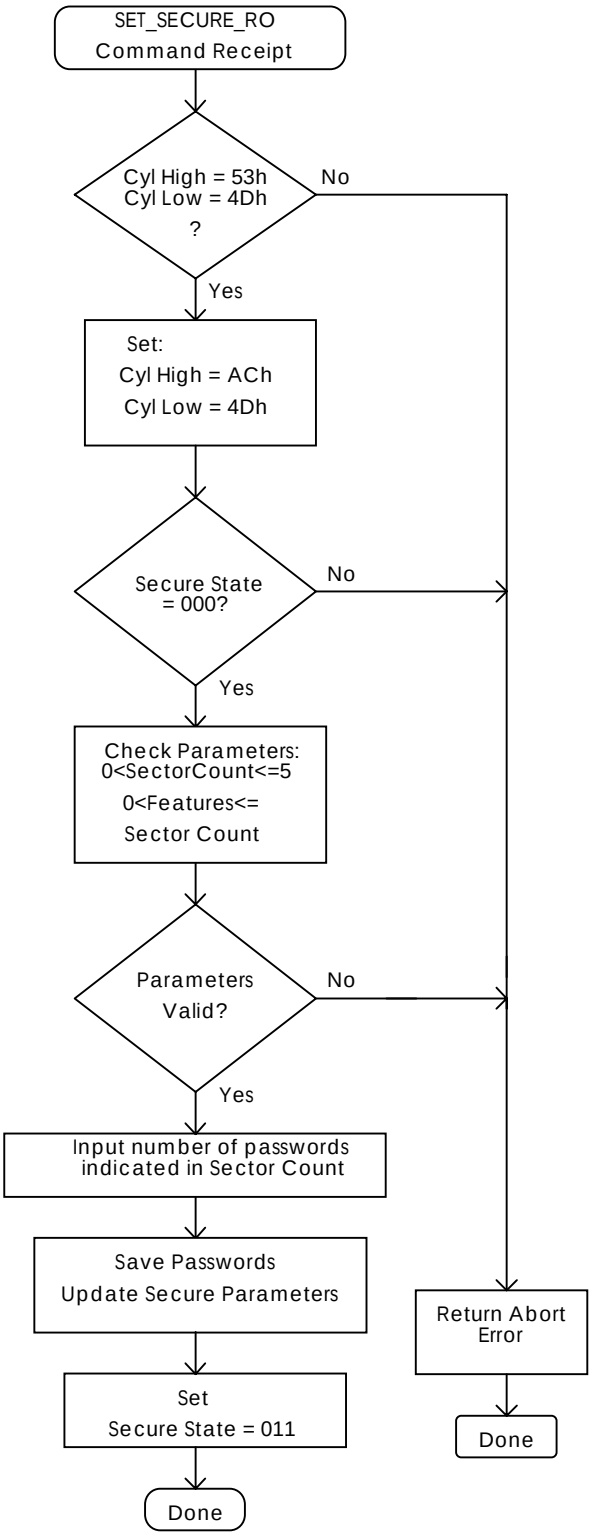

Figure 3 - SET_SECURE_RO Command Execution

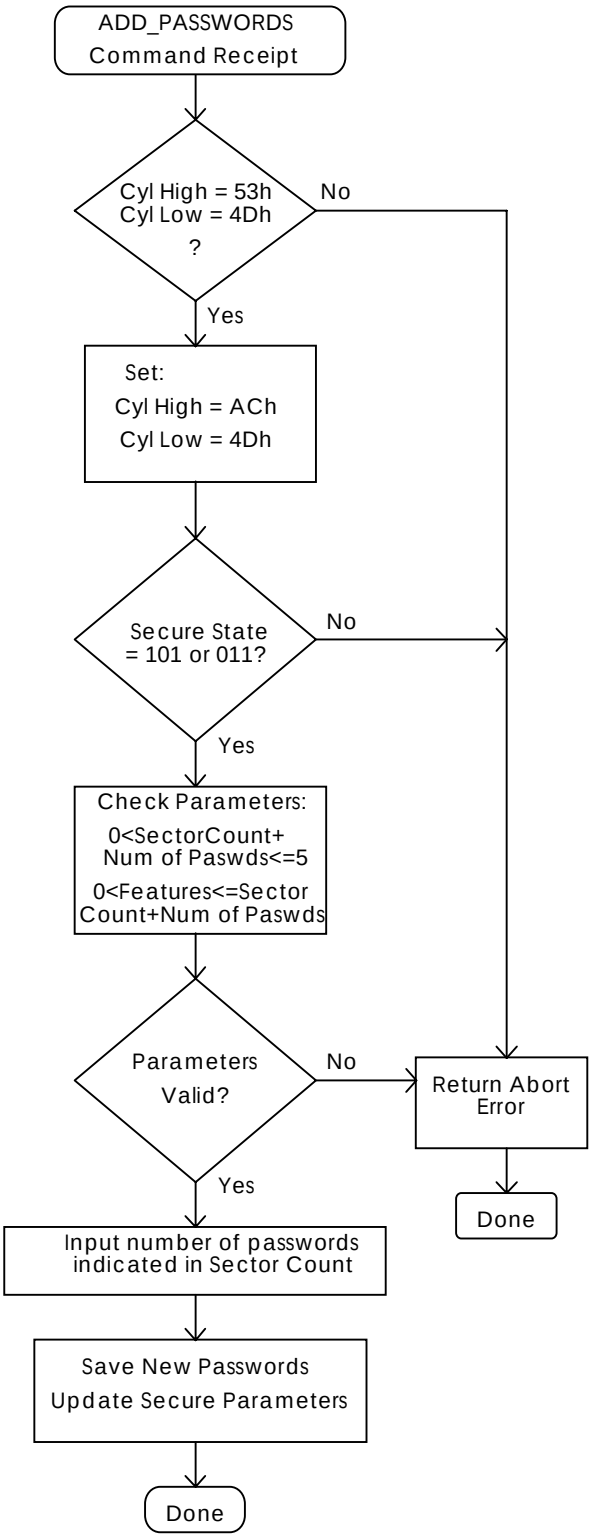

Figure 4 - ADD_PASSWORD Command Execution

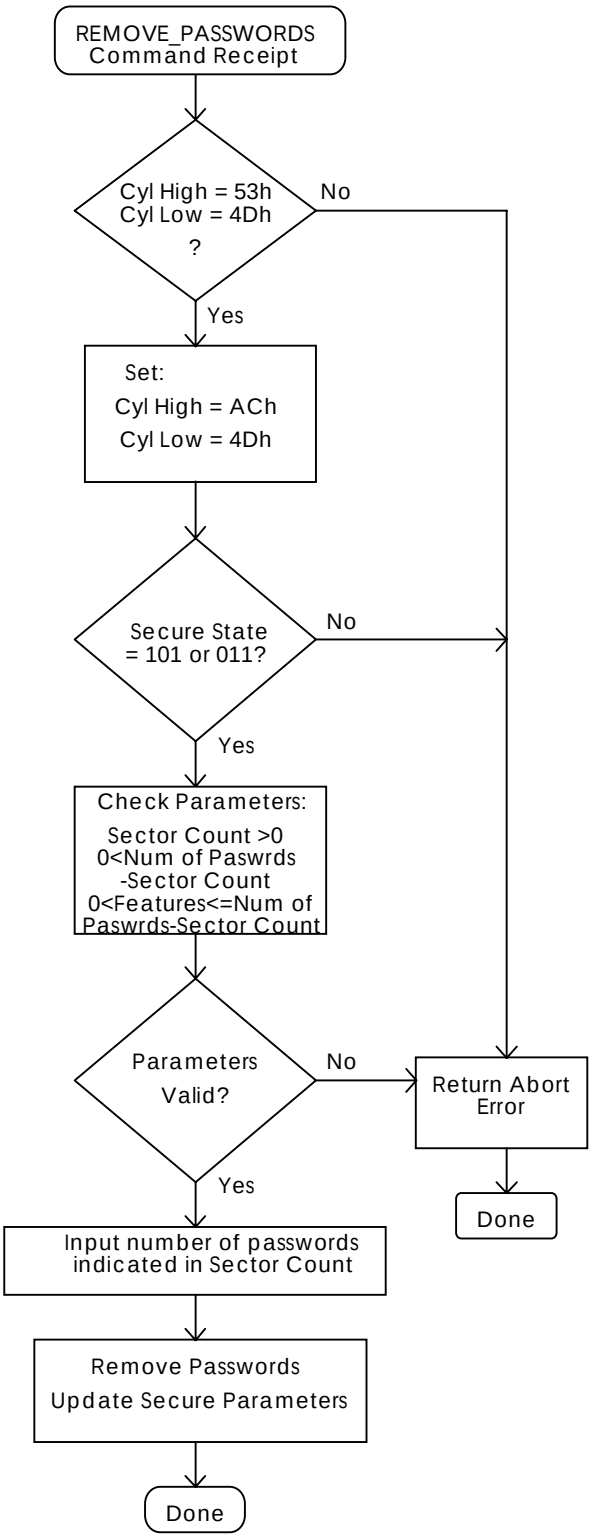

Figure 5 - REMOVE_PASSWORDS Command Execution

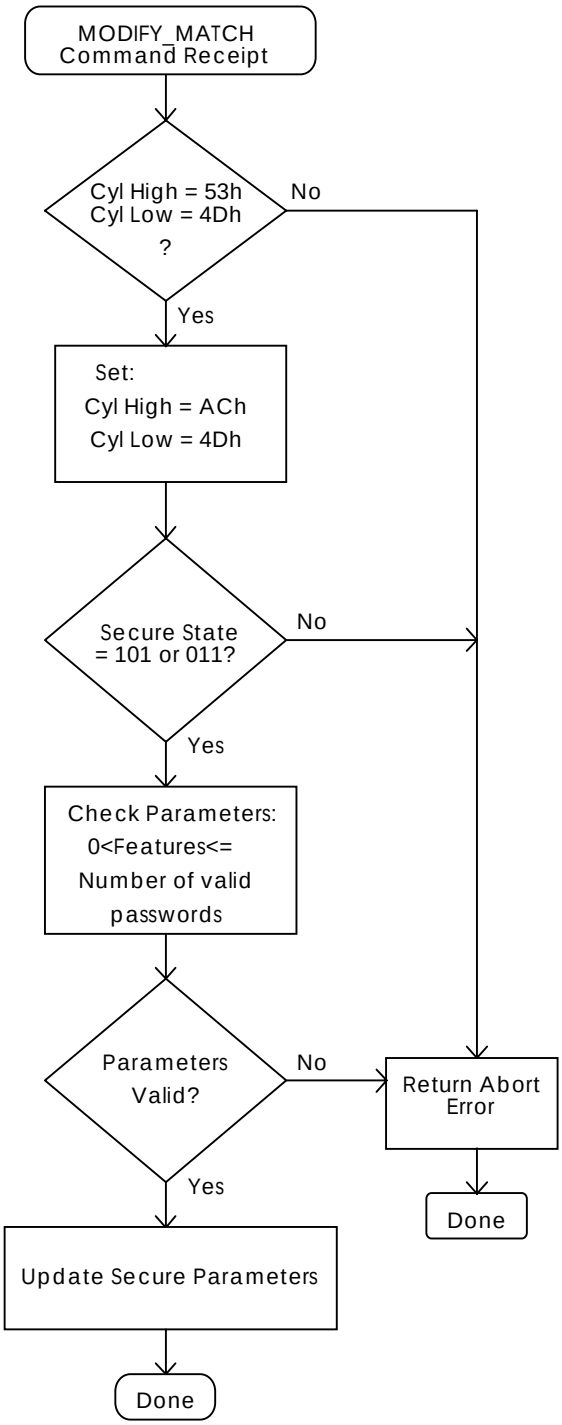

Figure 6 - MODIFY_MATCH Command Execution

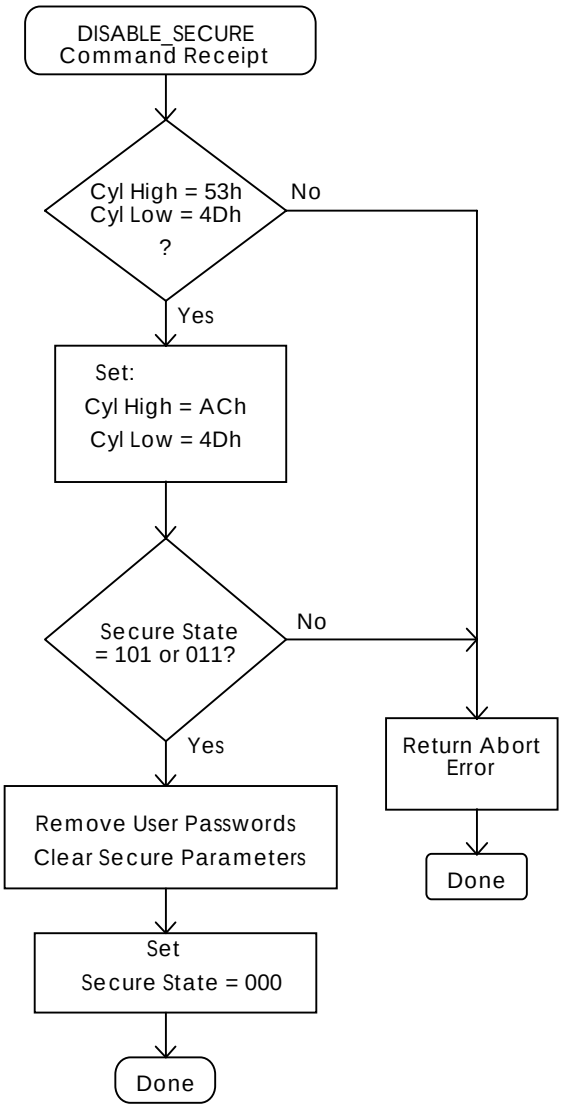

Figure 7 - DISABLE_SECURE Command Execution

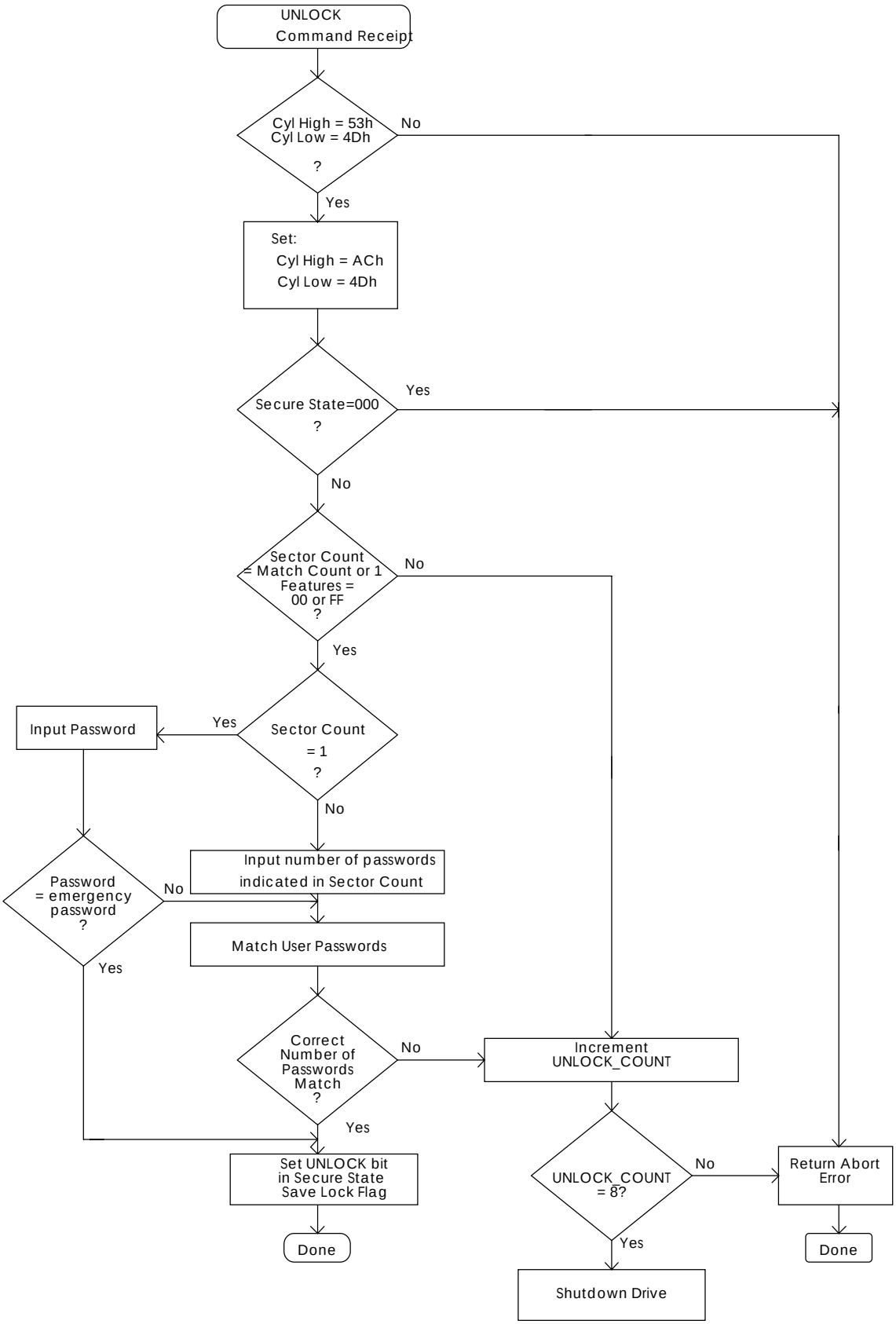

Figure 8 - UNLOCK Command Execution

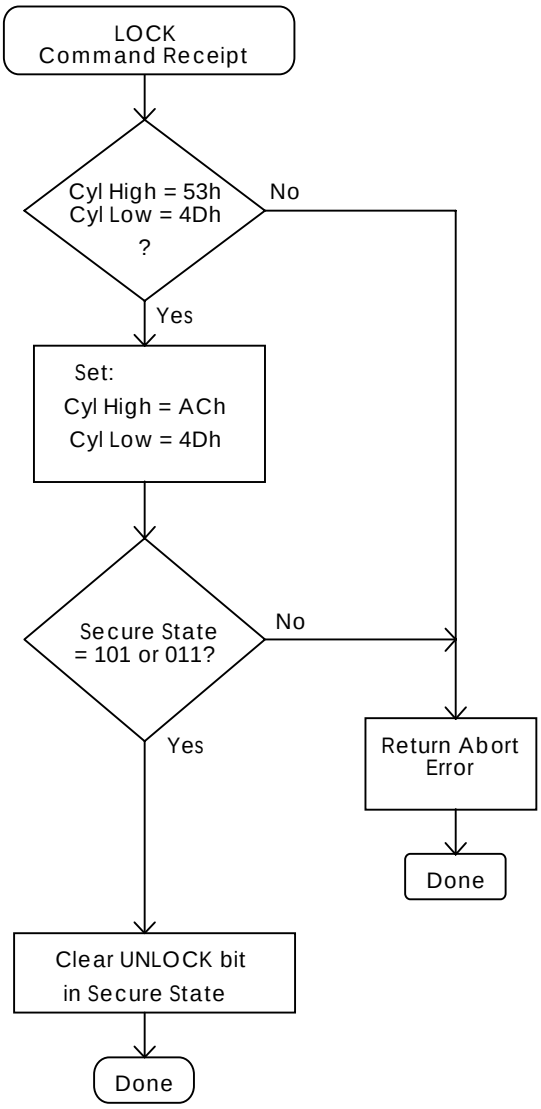

Figure 9 - LOCK Command Execution