Western Digital Technologies, Inc.
20511 Lake Forest Dr.
Lake Forest, Ca. 92630

To: **T10 CAP Working Group**
Contact: **Curtis E. Stevens**
Phone: 949-672-7933
Email: Curtis.Stevens@wdc.com
Date: **9-May-2007**

Subject: **Proposal to add Device Server Password Security to SPC-4**

1 Related documents

ATA8-ACS
SPC-4

2 Introduction

There are a variety of devices that are being bridge from a bus that uses a SCSI functional protocol to a bus that uses an ATA functional protocol. The SAT working group is defining methods for translating SCSI functions into ATA function sequences. This does not address the issue of translating ATA capabilities into SCSI. One ATA capability with no translation is the Security Feature Set. Many ATA devices have this capability, but systems are unable to take advantage of this level of security simply because they do not have access to the ATA capability. This purpose of this proposal is to enable password security as it is defined in ATA8-ACS.

3 Operational Model

3.1 Overview

The optional Security 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.

3.2 Passwords

3.2.1 Overview

The system has two types of passwords: User and Master.

3.2.2 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.

Device Server Password Security is enabled by setting a User password with the Set Password function. When Device Server Password Security is Enabled, the device is automatically Locked (i.e., access to user data on the device is denied) after a power-on reset is processed until the Unlock function completes successfully.

3.2.3 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 factory-installed Master password may be valid before an initial Set Password function has been successfully processed. A device may contain both a valid Master and a valid User password. Setting the Master password does not enable Security (i.e., does not Lock the device after the next power-on reset has been processed)

3.2.4 Master Password Capability

A device with Security enabled has two ways of using the Master password. This capability has values of 'High' or 'Maximum'.

When the Master Password Capability is set to High, either the User or Master password may be used interchangably. See table 1.

When the Master Password Capability is set to Maximum, the Master password cannot be used with the Disable Password function and Unlock function. The Erase Unit function, however, does accept either a valid User or Master password.

Table 1 — Interaction of Master Password Capability and Passwords (when Security is not frozen)

				Actions Taken by Security Commands		
Security Enabled	**Master Password Capability**	**Passwords Defined**	**Password Supplied**	**SECURITY ENABLE PASSWORD**	**SECURITY UNLOCK**	**SECURITY ERASE UNIT**
No	N/A	Master Only	Correct Master	N	N	P
No	N/A	Master Only	Not Valid	A	A	A
Yes	High	Master and User	Correct Master	P	P	P
Yes	High	Master and User	Correct User	P	P	P
Yes	Maximum	Master and User	Correct Master	A	A	P
Yes	Maximum	Master and User	Correct User	P	P	P

Key:

N - NOP, do nothing and return normal completion
A - Return command aborted
P - Process the command (if all validations pass) or return command aborted

3.3 Frozen Mode

The Freeze Lock function prevents changes to all Security states until a following power-on reset or hardware reset. The purpose of the Freeze Lock function is to prevent password setting attacks on the security system.

3.4 Inquiry data

Editor's Note 1: One bit of Inquiry data needs to be assigned to indicate that the device is currently locked by this capability.

3.5 VPD Page

Editor's Note 2: A VPD page needs to be defined which returns the current security mode and the master password identifier.

3.6 Security initial setting

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

3.7 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.

The Erase Unit function 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 does not match the user password previously set with the Set Password function, the device shall return command aborted.

If the Master Password Capability was set to High during the last Set Password function, the device shall accept the Master password and complete normally.

If the Master Password Capability was set to Maximum during the last Set Password function, the device shall return command aborted for the Unlock function or Disable Password function if the Master password is supplied.

3.8 Password Attempt Counter

The device shall have an password attempt counter. The purpose of this counter is to defeat repeated trial attacks. The counter shall be decremented while in state SEC4, whenever the Unlock function fails because of an invalid User or Master password.

Once the counter reaches zero, it shall not be decremented, and the PasswordAttemptCounterExceeded bit (VPD Page TBD shall be set to one, and the Unlock function and Erase Unit function shall be command aborted until after processing the next power-on or hardware reset.

The PasswordAttemptCounterExceeded bit shall be cleared to zero by processing a power-on or a hardware reset.

The counter shall be set to five (5) after a power-on or hardware reset.

3.9 Command Interraction with Device Server security

SPC

Table 2 — SPC Security Command Actions (part 1 of 2)

Command	Locked[a]	Unlocked or Disabled[b]	Frozen[c]
ACCESS CONTROL IN	Allowed	Allowed	Allowed
ACCESS CONTROL OUT	Allowed	Allowed	Allowed
CHANGE ALIASES	Allowed	Allowed	Allowed
EXTENDED COPY	Allowed	Allowed	Allowed

[a] State SEC4
[b] States SEC1 or SEC5
[c] States SEC2 or SEC6

Table 2 — SPC Security Command Actions (part 2 of 2)

Command	Locked[a]	Unlocked or Disabled[b]	Frozen[c]
INQUIRY	Allowed	Allowed	Allowed
LOG SELECT	Allowed	Allowed	Allowed
LOG SENSE	Allowed	Allowed	Allowed
MANAGEMENT PROTOCOL IN	Allowed	Allowed	Allowed
MANAGEMENT PROTOCOL OUT	Allowed	Allowed	Allowed
MODE SELECT(6) / MODE SELECT(10)	Allowed	Allowed	Allowed
MODE SENSE(6) / MODE SENSE(10)	Allowed	Allowed	Allowed
PERSISTENT RESERVE IN	Allowed	Allowed	Allowed
PERSISTENT RESERVE OUT	Allowed	Allowed	Allowed
READ ATTRIBUTE	Allowed	Allowed	Allowed
READ BUFFER	Allowed	Allowed	Allowed
READ MEDIA SERIAL NUMBER	Allowed	Allowed	Allowed
RECEIVE COPY RESULTS	Allowed	Allowed	Allowed
RECEIVE DIAGNOSTIC RESULTS	Allowed	Allowed	Allowed
RELEASE(6)/ RELEASE(10)	Allowed	Allowed	Allowed
REPORT ALIASES	Allowed	Allowed	Allowed
REPORT IDENTIFYING INFORMATION	Allowed	Allowed	Allowed
REPORT LUNS	Allowed	Allowed	Allowed
REPORT PRIORITY	Allowed	Allowed	Allowed
REPORT SUPPORTED OPERATION CODES	Allowed	Allowed	Allowed
REPORT SUPPORTED TASK MANAGEMENT FUNCTIONS	Allowed	Allowed	Allowed
REPORT TARGET PORT GROUPS	Allowed	Allowed	Allowed
REPORT TIMESTAMP	Allowed	Allowed	Allowed
REQUEST SENSE	Allowed	Allowed	Allowed
RESERVE(6) / RESERVE(10)	Allowed	Allowed	Allowed
SECURITY PROTOCOL IN	Allowed	Allowed	Conflict
SECURITY PROTOCOL OUT	Allowed	Allowed	Conflict
SEND DIAGNOSTIC	Allowed	Allowed	Allowed
SET IDENTIFYING INFORMATION	Allowed	Allowed	Allowed
SET PRIORITY	Allowed	Allowed	Allowed
SET TARGET PORT GROUPS	Allowed	Allowed	Allowed
SET TIMESTAMP	Allowed	Allowed	Allowed
TEST UNIT READY	Allowed	Allowed	Allowed
WRITE ATTRIBUTE	Allowed	Allowed	Allowed
WRITE BUFFER	Allowed	Allowed	Allowed

[a] State SEC4
[b] States SEC1 or SEC5
[c] States SEC2 or SEC6

SBC

Table 3 — SBC Security Command Actions

Command	Locked[a]	Unlocked or Disabled[b]	Frozen[c]
FORMAT UNIT	Conflict	Allowed	Allowed
ORWRITE	Conflict	Allowed	Allowed
PRE-FETCH (10)/(16)	Conflict	Allowed	Allowed
PREVENT ALLOW MEDIUM REMOVAL (Prevent=0)	Conflict	Allowed	Allowed
PREVENT ALLOW MEDIUM REMOVAL (Prevent<>0)	Conflict	Allowed	Allowed
READ (6)/(10)/(12)/(16)/(32)	Conflict	Allowed	Allowed
READ CAPACITY (10)/(16)	Conflict	Allowed	Allowed
READ DEFECT DATA (10)/(12)	Conflict	Allowed	Allowed
READ LONG (10)/(16)	Conflict	Allowed	Allowed
REASSIGN BLOCKS	Conflict	Allowed	Allowed
START STOP UNIT with START bit set to one and POWER CONDITION field set to 0h	Conflict	Allowed	Allowed
START STOP UNIT with START bit set to zero or POWER CONDITION field set to a value other than 0h	Conflict	Allowed	Allowed
SYNCHRONIZE CACHE (10)/(16)	Conflict	Allowed	Allowed
VERIFY (10)/(12)/(16)/(32)	Conflict	Allowed	Allowed
WRITE (6)/(10)/(12)/(16)/(32)	Conflict	Allowed	Allowed
WRITE AND VERIFY (10)/(12)/(16)/(32)	Conflict	Allowed	Allowed
WRITE LONG (10)/(16)	Conflict	Allowed	Allowed
WRITE SAME (10)/(16)/(32)	Conflict	Allowed	Allowed
XDREAD (10)/(32)	Conflict	Allowed	Allowed
XDWRITE (10)/(32)	Conflict	Allowed	Allowed
XDWRITEREAD (10)/(32)	Conflict	Allowed	Allowed
XPWRITE (10)/(32)	Conflict	Allowed	Allowed

[a] State SEC4
[b] States SEC1 or SEC5
[c] States SEC2 or SEC6

3.10 Device Server Security State Transition

See ATA8-ACS Security States for the state transition diagram associated with this function.

4 ATA Device Server Password Security description

4.1 Overview

the ATA Device Server Password Security functions use the SECURITY PROTOCOL SPECIFIC field as shown in table 4. Table 5 described the security functions..

Table 4 — Device Server Password Security

Bit Byte	7	6	5	4	3	2	1	0
0	OPERATION CODE (B5h)							
1	SECURITY PROTOCOL (EFh)							
2	Reserved				SECURITY FUNCTION			
3	Reserved							
4	INC_512							
5	Reserved							
6	(MSB)			TRANSFER LENGTH				
9								(LSB)
10	Reserved							
11	Control							

Table 5 — Device Server Password Security functions

SECURITY FUNCTION	Description	ATA Command
0h	Reserved	
1h	Set Password	SECURITY SET PASSWORD
2h	Unlock	SECURITY UNLOCK
3h	Erase Prepare	SECURITY ERASE PREPARE
4h	Erase Unit	SECURITY ERASE UNIT
5h	Freeze Lock	SECURITY FREEZE LOCK
6h	Disable Password	SECURITY DISABLE PASSWORD
7h-Fh	Reserved	

4.2 Set Password

Shall transfer 1 512 byte block of data as defined in .table 6. Set the master or user password. See the ATA8-ACS SECURITY SET PASSWORD command for a description of this function.

Table 6 — Set Password Data

Bit Byte	7	6	5	4	3	2	1	0
0	Reserved							HM
1	Reserved							UM
2	(MSB)			PASSWORD				
33								(LSB)
34	(MSB)			MASTER PASSWORD IDENTIFIER (Only valid if UM=1)				
35								(LSB)
36	Reserved							
511								

HM shall be set to zero to place the drive in High security mode. HM shall be set to one to place the drive in Maximum security mode.

UM shall be set to zero to set the User password. UM shall be set to one to set the Master password.

PASSWORD is a 32 byte binary value.

MASTER PASSWORD IDENTIFIER is a 16 bit value

4.3 Unlock

Shall transfer one 512 byte block of data as defined in table 6. See the ATA8-ACS SECURITY UNLOCK command for a description of this function.

4.4 Erase Prepare

Shall preceed erase unit. Shall not transfer data. See the ATA8-ACS SECURITY ERASE PREPARE command for a description of this function.

4.5 Erase Unit

Shall transfer one 512-byte block of data as defined in table 7. See the ATA8-ACS SECURITY ERASE UNIT command for a description of this function.

Table 7 — Erase Unit Password Data

Bit Byte	7	6	5	4	3	2	1	0
0	Reserved							EM
1	Reserved							UM
2	(MSB)	PASSWORD						
33								(LSB)
34	Reserved							
511								

EM shall be set to zero to request a Normal mode erase. EM shall be set to one to request an Enhanced Mode erase.

UM shall be set to zero to compare the User password. UM shall be set to one to compare the Master password.

PASSWORD is a 32 byte binary value.

4.6 Freeze Lock

Prevent changes to the security system. shall not transfer data. See the ATA8-ACS SECURITY FREEZE LOCK command for a description of this function

4.7 Disable Password

Shall transfer one 512-byte block of data as defined in table 8. See the ATA8-ACS SECURITY DISABLE PASSWORD command for a description of this function.

UM shall be set to zero to compare the User password. UM shall be set to one to compare the Master password.

PASSWORD is a 32 byte binary value.

Table 8 — Disable Password Data

Bit / Byte	7	6	5	4	3	2	1	0
0	Reserved							
1	Reserved							UM
2	(MSB)							
33	PASSWORD							(LSB)
34	Reserved							
511								