An Initial outline the SCSI interface requirements for IEEE P1667

To: **T10 Technical Committee**
From: **Avraham Shimor**
M-Systems Flash Disk Pioneers Ltd
for the IEEE P1667 Workgroup (Standard Protocol for Authentication in Host Attachments of Transient Storage Devices)
7 Atir Yeda Str
Kfar Saba, ISRAEL 44425
Phone: +972 9 764 5106
Fax: +972 3 548 8666
Email: Avraham.Shimor@m-systems.com
Date: **March 8, 2006**

1 Introduction

The purpose of this contribution is to outline the SCSI interface requirements for enabling support of the P1667 protocols and command and result data streams. As the IEEE P1667 Specification (Standard Protocol for Authentication in Host Attachments of Transient Storage Devices) has not yet been publicly released at this time, this document is submitted to T10 for information only, in order to enable and stimulate an initial discussion on the subject.

Attached to this contribution is an extract from the evolving P1667 Specification (T10/06-112r0), focusing on the topics relevant to an eventual implementation of this standard over a SCSI interface, which can be used by the members of T10 to have an initial insight into the concepts and ideas underlying P1667.

A similar contribution was presented to T13, with the general intention for both T10 and T13 to define and use similar command 'containers' or conduits, possibly relying upon the Security Protocol In/Out (previously designated as Trusted In/Out) as are being defined by the Trusted Computing Group (TCG).

2 Outline of Requirements

The P1667 standard is based upon a flexible and extensible collection of underlying protocols. Therefore, the command set implementation must support the following mechanism for detection an discovery of the particular set of functional and interface capabilities supported by any particular host-device configuration. P1667 requests the guidance of T10 to determine which of the following mechanisms will be more favorably accepted by T10:

1) Determination of SECURITY PROTOCOL support by INQUIRY command with the allocation of a reserved bit in the first 36 bytes.
2) Determination of SECURITY PROTOCOL support by use of the INQUIRY command with the allocation of a reserved bit after the first 36 bytes and the allocation of a bit in the first 36 bytes specifying that all 256 bytes of the INQUIRY command response must be read.
3) "Blind probe" for SECURITY PROTOCOL support by sending the SECURITY PROTOCOL IN command with a Security Protocol ID of 00h to retrieve the list of supported security protocols.

Note: Options 1 and 2 are functionally identical to the corresponding T13/ATA mechanism, where the ATA command IDENTIFY DEVICE is used in the same context and purpose as proposed here for the SCSI INQUIRY.

2.1 Elaboration of Option 1:

This option is most favored by the IEEE 1667 standard committee as it provides the greatest simplicity and level of commonality with the proposal presented to T13 for ATA support of IEEE 1667. At this time T13 will not approve use of blind probing for protocol support.

- First, the SCSI INQUIRY command shall be used to discover whether or not the SECURITY PROTOCOL feature set is supported, and if it is supported, whether or not it is enabled. A bit in the initial 36 bytes of the INQIRY command response will be allocated by T10 to indicate support for SECURITY PROTOCOL.

- If the SECURITY PROTOCOL support bit is set the SECURITY PROTOCOL IN command is used to return the list of supported SECURITY PROTOCOLS. This list is examined for the inclusion of the 1667 PROTOCOL identifier.

- If the P1667 PROTOCOL identifier is found, then the actual set of commands and capabilities supported by a certain device/host instance will be determined using IEEE 1667 specific values..

2.2 Elaboration of Option 2:

This option is similar to Option 1 but allows for the allocation of the bit used to indicate SECURITY PROTOCOL support after the first 36 bytes of the INQUIRY command response. Instead a bit will be allocated in the first 36 bytes of the INQUIRY command response to indicate that all 256 bytes of the INQUIRY command response must be read. Alternatively, hosts which support IEEE 1667 may be required to read always all 256 bytes of the INQUIRY command response..

- First, the SCSI INQUIRY command shall be used to discover whether or not the SECURITY PROTOCOL feature set is supported, and if it is supported, whether or not it is enabled. A bit in the initial 36 bytes of the INQIRY command response will be allocated by T10 to indicate that all 256 bytes of the INQUIRY command response must be read.

- If the bit indicating a full read of the INQUIRY command response is set the INQUIRY command will be repeated will all 256 bytes returned by the command being read. A bit after the initial 36 bytes of the INQIRY command response will be allocated by T10 to indicate support for SECURITY PROTOCOL.

- If the SECURITY PROTOCOL support bit is set the SECURITY PROTOCOL IN command is used to return the list of supported SECURITY PROTOCOLS. This list is examined for the inclusion of the 1667 PROTOCOL identifier.

- If the P1667 PROTOCOL identifier is found, then the actual set of commands and capabilities supported by a certain device/host instance will be determined using IEEE 1667 specific values..

2.3 Elaboration of Option 3:

This option is consistent with the current direction taken by the definition of SECURITY PROTOCOL in that it relies on sending a SECURITY PROCOL command without first determining that SECURITY PROTOCOL is supported. The use of this mechanism will complicate the acceptance of IEEE 1667 as developers will need to distinguish between SCSI based interfaces and ATA based interfaces since T13 has rejected the use of this mechanism in ATA.

- The SECURITY PROTOCOL IN command is used to request the list of supported SECURITY PROTOCOLS. Failure of the command indicates lack of support for SECURITY PROTOCOL and by implication the lack of support for IEEE 1667.

- If this command succeeds the list is examined for the inclusion of the 1667 PROTOCOL identifier.

- .If the 1667 PROTOCOL identifier is found the actual set of commands and capabilities supported by a certain device/host instance will be determined using IEEE 1667 specific values..

It is the intention that the Security Protocol In/Out commands, as introduced by TCG, shall be used as the conduit for implementing the particular P1667 commands, while using a specific Protocol ID dedicated/assigned to identify P1667.

The 1667 commands shall be based on the Security Protocol In/Out command conduit.