

# Media Management System Requirements

## Working Draft 5.2

### IEEE Storage System Standards Working Group

January 30, 1998

The purpose of this document is to list requirements for the Media Management System (MMS), a set of IEEE standards that are being developed by the IEEE Storage System Standards Working Group. This document serves to guide the P1244 standards development effort. It is not intended to guide outside efforts, or to serve as an absolute set of requirements for the standards. These requirements can be reasonably implemented, and will be of value to a wide range of users. They are neither abstract goals, nor complex standards of use only to a small group of elite users.

*Media management* refers to automated or manual operations involving physical storage media (disks, tapes, or other media).

Certain portions of the MMS standard are *mandatory* — systems not meeting the requirements of mandatory portions of the specifications are not compliant with the standard. Other portions of the specifications are *optional* — systems may either fully implement or not implement optional components. Options may be *grouped* — if any option in a group is implemented, all must be implemented.

Certain requirements must be met by *plug-ins*. Plug-ins are site-supplied modules to implement local policies. Plug-ins shall be clearly identified as non-standard in distributed source code and documentation. Plug-ins shall not change the operation of standard components nor will they require non-standard operation of other components.

## 1. Definitions

See the definitions in the MMS Architecture document (1244.1).

## 2. Interface Requirements

2.1. There shall be one client interface to the MMS, through which all requests are received.

2.2. The MMS shall provide authentication mechanisms to restrict access.

- Optional — There may be subsets of service or administrator requests to allow additional access restrictions.
- Authentication mechanisms shall include the reporting of authentication failures to administrative personnel.

2.3. The MMS interface shall be asynchronous (non-blocking); acceptance of a new command shall not require prior receipt of the result of a previous command.

- Optional — Specific commands or implementations may *execute* synchronously, although asynchronous execution is desirable for efficiency.

- 2.4. Mechanisms shall be provided to make resources available for use (“ready”). This is independent of mechanisms used to reserve the resources for use. For example, cartridges stored off site may have to be moved to a library before they can be mounted.
- 2.5. The MMS shall utilize underlying operating systems or other external mechanisms to allow client access to data paths. The MMS is not on the data path, although the MMS may use protected data paths to implement label creation and checking. IEEE standard movers, if they exist, are not part of the MMS.
- 2.6. Responses to clients shall include the result of the action requested (success or failure) and additional information as requested, such as the drive on which a cartridge was mounted, or information describing encountered errors.
- 2.7. Error responses shall be of standard format to enhance portability, shall reflect the cause of errors to a reasonable level of detail, and shall contain both machine- and human-readable sections. Additional (linked) error returns for a single function are permitted to increase detail, with fundamental errors specified in the standard to enhance portability.
  - 2.7.1. The MMS shall contain three or more levels of error reporting. MMS interfaces shall contain mechanisms for the client to specify the level of error reporting desired.
    - Specific Report — Simple error report of detected hardware or software error. The report shall include the failing hardware, the detecting software module, and the type of error (e.g., “read error” or “SCSI timeout”).
    - Contextual Report — In addition to the information provided in the specific report, client information, the operation in progress, and the possible consequences of the failure are included.
    - Recovery Report — In addition to the information provided in the contextual report, the performed or recommended error recovery shall be described.
  - 2.7.2. Optional — The MMS may accommodate administrative policy plug-ins to:
    - Control which principals have priority to access resources when there are conflicting or overlapping requests.
    - Control the delayed allocation of resources.
    - Resolve deadlocks.
    - Exploit delayed dismounts.
- 2.8. **Cartridge Mounts**
  - 2.8.1. A mount consists of moving a cartridge to a drive and readying the media for access to access a specified partition. The MMS shall be able to verify external and internal labels if they exist and, if possible, shall protect the integrity of internal labels and shall protect cartridge partitions not specified by the mount from read or write access.
    - 2.8.1.1. The MMS shall include provisions for pluggable internal-label verifiers to accommodate standard and non-standard label formats.

- 2.8.2. The MMS shall support site-supplied plug-ins to automatically identify labeled cartridges introduced manually via a library port.
- 2.8.3. The MMS shall allow an application to indicate future requirements for volumes, drives, or other resources. The indication may be used to ensure that resources are available, to reserve (lock) resources, or to achieve efficient use of resources.
- 2.8.4. Mount requests may specify one or more volumes. The MMS shall provide flexibility regarding how these mount requests are specified and executed, by allowing an atomic mount of any  $n$  volumes from a group of  $m$  volumes ( $m \geq n$ ). For example:
- Mount a single volume.
  - Simultaneously mount the specified volumes in an atomic manner.
  - Mount any one of a number of specified volumes.
  - Mount any subset of a number of specified volumes.
- Note: The MMS is not required to handle atomic mounts involving multiple MMSs. If such mounts are needed by a client application, that application shall coordinate the individual MMSs.
- 2.8.5. When there are multiple drives of the same type, clients shall be able to specify the particular drive to be used, a set of acceptable drives, or a set of unacceptable drives. When more than one drive is acceptable for a particular mount, the MMS shall be capable of selecting a drive based on:
- Mount efficiency (e.g. the closest drive).
  - Drive history (e.g. the drive with the fewest number of mounts).
  - Resource efficiency (e.g. when drives have different capabilities).
  - Other factors specified by the system administrator.
- 2.8.6. In a manual system, the human operator shall be able to mount the cartridge on any acceptable drive. The identification of labeled cartridges mounted by human operators shall be automatic with no manual operation required other than physically mounting the cartridge.
- 2.8.7. The MMS shall allow a human operator to mount a cartridge in a drive without a pending mount request by the MMS. Mechanisms shall be present to ensure appropriate resource utilization.
- 2.8.8. There shall be mechanisms to order mount requests based on client-specified priorities (ordering their own mounts), and client or other priorities specified by system administrators. The MMS shall provide sufficient information so that priorities can be adjusted by site-supplied administrative applications.
- 2.8.9. The MMS shall include mechanisms that enable clients and administrators, with appropriate authentication:
- To display the contents of the mount queue.

- To delete queued requests.
- To change the priority of queued requests.

## 2.9. Cartridge Dismounts

2.9.1. The MMS shall be capable of removing cartridges from drives, with the following options (when supported by the robotic system):

- The cartridge is returned to the storage location from which it was mounted (e.g. to a “home” location).
- The cartridge is moved to a location based on dismount efficiency (e.g. the closest slot).
- The cartridge is moved to a location accessible to a human operator.

2.9.2. The MMS shall be capable of keeping cartridges mounted after dismount commands are received in anticipation of additional accesses for these cartridges. Criteria for dismounting such cartridges shall include:

- When drives are needed.
- When the number of available drives has reached an administrator-specified minimum.
- When priority or time-out mechanisms indicate that cartridges should be dismounted.

## 2.10. Cartridge Transfers

2.10.1. The MMS shall support the transfer of cartridges between libraries. Such transfers may be invoked:

- Automatically when required to mount a cartridge.
- On a policy basis — for example, to move a cartridge from an automated library to a vault based on site-defined criteria.
- When a human operator decides to move a cartridge.

2.10.2. The MMS architecture shall not preclude mechanisms to transfer cartridges between off-line MMSs or between MMSs and other cartridge-management systems (e.g. MVS).

## 3. Interoperability Requirements

3.1. The MMS collection of standards shall define the interoperability constraints and parameters for MMS-compliant systems. These standards will specify the necessary languages, character sets, syntax, and semantics for interoperability with the MMS and its components.

3.2. The MMS shall use widely accepted standards, such as TCP/IP for communication.

3.3. While MMS implementations may be proprietary and can depend on other proprietary systems, the interoperability of such implementations with other MMS implementations must not require additional third-party proprietary software.

## 4. Reliability Requirements

- 4.1. The MMS shall verify and consistency-check human and mechanical operations when the underlying hardware and operating system provide the means to do so. Such mechanisms shall include redundant checks where appropriate. For example, at the time a volume is mounted, the MMS may check both an external label and an internal label and may verify that the operating system has access to the volume through its drive interface.
- 4.2. The MMS design shall emphasize automatic recovery of errors where technically feasible.
  - 4.2.1. Error and message logging of the MMS shall be sufficiently flexible to allow the identification of failed or failing components, the performance analysis of MMS processes, the tracking of MMS usage for accounting purposes, the tracking of resource status, and to allow system administrator to monitor the MMS (ala Unix syslogd).
  - 4.2.2. The MMS shall provide mechanisms to operate the system in degraded modes. For example, the MMS may permit manual cartridge mounts in case of automated library failure.
  - 4.2.3. Failure of hardware not in a critical access path shall not disable the MMS.
  - 4.2.4. The MMS shall contain mechanisms to detect and recover from situations in which the mount queues are stalled because particular jobs are encountering errors.
- 4.3. The MMS shall utilize backup mechanisms, redundancy, or other mechanisms to guard against loss of metadata through hardware or software failure, human error, or natural disaster.
  - 4.3.1. There shall be mechanisms to recover normal operation after the permanent loss of all metadata, for example by auditing robotic devices and/or reading internal or external label information. It is recognized that not all dynamic metadata can be recovered by this means; in the extreme, such recovery may be equivalent to the initial installation of the MMS.
    - 4.3.1.1. MMS implementations shall specify what configuration and other information is critical, and shall specify the consequences of losing this information and shall recommend backup procedures to safeguard it.
  - 4.3.2. The MMS shall include repair mechanisms to recover from unanticipated database errors—data corruption short of a disaster.
  - 4.3.3. The MMS shall utilize atomic transactions or other mechanisms to maintain metadata consistency (e.g., each cartridge is shown to be in only one place at a time).
- 4.4. The MMS shall contain library start-up algorithms to initialize the state and location of cartridges, possibly left in a drive or robotic device, without manual intervention if technically possible. The MMS shall be capable of moving cartridges, if necessary, to allow a complete audit.
- 4.5. The MMS shall contain mechanisms to investigate apparently duplicate cartridges when, for example, it finds a cartridge in one location while the metadata indicates that the same

cartridge is elsewhere. Manual intervention will be required only after the MMS has found unequivocal evidence of duplicate cartridges.

- 4.5.1. Duplicate cartridges (those with identical external or internal labels) shall not be allowed. MMS implementations shall describe the actions required to resolve the existence of duplicates.

## **5. Extensibility Requirements**

- 5.1. The MMS shall include plug-in mechanisms to allow MMS vendors to differentiate their products through non-standard functionality. Such functionality shall meet the requirement that plug-ins be clearly identified and that they not change the operation of standard components.
- 5.2. The MMS shall provide mechanisms to allow clients to utilize multiple physical resources (e.g. cartridges and drives) simultaneously.
  - 5.2.1. The MMS shall contain mechanisms to allow clients to reserve resources to avoid deadlock. In addition, the MMS shall perform deadlock detection when possible.
- 5.3. The MMS shall not preclude the use of existing data transfer mechanisms, including parallel I/O to striped media and network-attached peripherals.
- 5.4. The MMS shall support mounts performed by robotic devices and by human operators. The MMS architecture shall not rule out simple SCSI robots, robots for video media, or complex, high-end robotic systems.
- 5.5. The MMS shall support multiple cartridge types and multiple drive types, and shall be capable of mounting cartridges only on drives of the appropriate types. Consideration shall be given to various media characteristics, including physical form factor, physical tape type, tape size, and bit encoding format.
- 5.6. The MMS shall be designed to support the addition of new types and instances of drives and robotic devices, ideally without interrupting service to existing clients and components.
  - 5.6.1. The MMS architecture shall not limit the efficient use of current or anticipated automated libraries, drives, media types, redundant control paths, etc.
  - 5.6.2. There shall be no architectural or practical limits placed on the number of cartridges, drives, or robotic devices that can be supported.
  - 5.6.3. There shall be separate interfaces for drives and robotic devices.
  - 5.6.4. The MMS shall include provisions for plugable robot and drive managers.
  - 5.6.5. Optional — The ability to change the MMS configuration, e.g. add new drives, without interrupting operation of other devices is highly desirable.

## **6. Configuration Requirements**

- 6.1.1. The MMS may include mechanisms to allow clients or system administrators to configure the MMS to comply with site policies. Such policies may include:

- Authentication and authorization mechanisms, except that the MMS shall not compromise existing operating system security mechanisms.
  - Priority and scheduling policies: Client priorities (individual or group priorities), time-dependent priorities (older requests receive priority), and fair-share scheduling (to prevent clients from monopolizing resources).
  - Inactive volume dismount and other time-out policies.
  - Policies on the forcible dismount of active volumes, if this is supported by the underlying system software.
  - Resource reservation policies and limits.
- 6.1.2. The MMS shall include monitoring, logging, audit trail, and reporting mechanisms designed to allow external applications to:
- Monitor the current state of the MMS on demand. The information supplied shall be adequate to detect failed components, identify bottlenecks, identify clients using the MMS, and identify the state of all resources managed by the MMS.
  - Track down problems. Notification mechanisms shall be provided to bring required maintenance or problems detected by the MMS to the attention of maintenance or administrative personnel. These mechanisms may provide information to be polled.
  - Generate usage statistics.
  - Charge for delivered services.

## **7. Media Requirements**

- 7.1. The intent of these requirements is to include non-removable media, media stored in vaults, and media stored in libraries.
- 7.2. The MMS shall be able to handle media with and without internal or external labels.
- 7.3. The MMS shall have mechanisms to aid in internally labeling unlabeled media.
- 7.4. The MMS shall include mechanisms to create partitions within media cartridges on which the partition concept is supported by the hardware.
- 7.5. The MMS shall be capable of supporting the concept of scratch pools and other media groups (RAIT).

## **8. Metadata Requirements**

- 8.1.1. The MMS shall maintain metadata describing the objects it controls, such as volumes, cartridges, drives, automated libraries, and vaults. The purpose of this metadata is to identify, locate, and track the history of these objects. The specific metadata required for each object will include the following:
- Identification information, including machine-oriented information (e.g. internal labels or bar codes from external labels), and human-oriented information (e.g. other external label information, comments).

## Media Management System Requirements

- Physical descriptive information, such as the cartridge types supported, cartridge form factor, media type and manufacturing batch, tape length, bit encoding format, densities supported, etc.
  - Ownership information, including the authentication information required for access.
  - Object history, such as the date and time the object was placed into service, the number of times accessed, the dates, times, and other details of recent accesses, error history, and maintenance information.
  - The current physical location of the object.
  - The configuration of the object, if applicable. Library configuration, for example, shall include the type and location of drives, input/output ports, and attachments to other libraries, topology information, including slots, cartridge type supported, import/export capabilities, cartridge identification information for each occupied logical or physical location, host connectivity, etc.
  - The current status of the object — removed from service, operation in progress, available for use, error or degraded state, ID of clients being served, other objects being accessed, etc.
- 8.2. The MMS shall support client-specified name/value metadata pairs, limited in number only by the available hardware. The MMS may pre-define some such pairs. Client-defined metadata pairs shall persist until explicitly removed or until the objects to which they are attached are removed. There may be administrative limits placed on metadata pairs.
- 8.3. Query mechanisms shall be provided to allow client-defined subsets of metadata to be accessed.
- 8.4. The MMS interface shall include authenticated mechanisms for clients to view, add, revise, and delete metadata as appropriate. The MMS shall be capable of importing and exporting metadata with cartridges to facilitate moving cartridges between MMSs and to initialize metadata for incoming blank or pre-recorded media. This may be accomplished via communications between MMSs.