A Proposal for Access Controls (aka SAN Boxes)

T10/99-278 revision 4

(Apropos T10/99-245r8)

Jim Hafner
IBM

May 17, 2000

Outline of talk

- Overview of changes in 99-245r8
- Summary of Service Actions
- Summary of ASC/ASCQs
- Open Questions

Major Changes from 99-245r5

- Change of LUN Map owner from target to PAM (rev6)
- Proxy Tokens are now non-volatile (rev6)
- iLUN term goes away, now use "default LUN"(rev6)
- Major rewrite of the Model clause (for clarity; rev8)
  - removal of term "LUN Mapping" though the function is still there
- Revised wording of proposed changes to EXTENDED COPY to support proxy model (rev8)
- "access controls coordinator" reported in INQUIRY data (rev7); AC IN/OUT cmds to any LUN with ACC=1 (rev8)
- New timer-based model for blocking override of "Key" (rev7)

Major Changes from 99-245r5 *(continued)*

- Cleaned up service actions (rev7-8)
  - removed unnecessary ones
  - moved all "configure" to OUT and "report" to IN
- Changes to MANAGE ACL (rev8)
  - removed some Page Codes for MANAGE ACL
  - Change in ACL entry is "add, remove or replace"
  - Initiator goes "not-enrolled" if ACL change, with exceptions
- Expanded on Access Controls Log (rev7-8)
  - Key Override events
  - Invalid Key events
  - Enrollment triggered LUN Map conflicts (ACL Conflict)
- Cleaned up glossary changes (rev8)

Major Changes from 99-245r5 *(continued)*

- Any Allocation Length is OK in IN cmd (rev8)
- Parameter List Length of zero is OK in OUT cmd (rev8)
- Removed Process Associator from FCP TransportID (rev8)
- ACL Conflict (LUN Map problem) fails completely (rev8)
- Clarified behavior of all service actions when access controls are disabled (rev8)
- Closed on "Supported LUN-Mask Format" (rev8)
- Closed on REPORT LU DESCRIPTORS format (rev8)
- Plagarized Ralph's wording for "interactions of access controls and other features" (rev8)
- Changed "de-enrolled" to "pending-enrolled" (rev8)

Stuff that stayed from rev5

- Configuration of (non-proxy) ACs requires "Management Identifier Key" shared between configuring application client and device
- Proxy ACs still available (revised model)
- Access granted with
  - AccessID identifier (as enrolled by initiator)
  - TransportID identifier (e.g., FC-WWN, now only persistent identifier)

Proposed Service Action Summary (IN)

- **REPORT ACL** (mandatory)
  - for PAM to get current state (including outstanding Proxy Tokens)
- **REPORT LU DESCRIPTORS** (mandatory)
  - for PAM to get inventory data (default LUN list, READ CAPACITY, IDENTIFIER, etc)
- **REPORT ACCESS CONTROLS LOG** (mandatory)
  - for PAM to get to access controls log
- **REPORT OVERRIDE LOCKOUT TIMER** (mandatory)
  - for PAM to get current timer status
- **REQUEST PROXY TOKEN** (optional)
  - for host to get Proxy Token for third party functions

Proposed Service Action Summary (OUT)

- **MANAGE ACL** (mandatory)
  - for PAM to manage ACL data
- **DISABLE ACCESS CONTROLS** (mandatory)
  - for PAM to shut down all ACLs (factory default)
- **ACCESS ID ENROLL** (mandatory)
- **CANCEL ENROLLMENT** (mandatory)
  - for host to gain access and release access to LUs by AccessID
- **CLEAR ACCESS CONTROLS LOG** (mandatory)
  - for PAM; except for Key Override portion
- **MANAGE OVERRIDE LOCKOUT TIMER** (mandatory)
  - restart (by any initiator) or reconfigure (by PAM) the Override Lockout Timer

Proposed Service Action Summary (OUT) *(continued)*

- **OVERRIDE MGMT ID KEY** (mandatory)
  - replace "lost" key (must not be blocked by timer)
- **REVOKE PROXY TOKEN** (optional)
- **REVOKE ALL PROXY TOKENS** (optional)
  - for host to invalidate one or all Proxy Tokens
- **ASSIGN PROXY LUN** (optional)
- **RELEASE PROXY LUN** (optional)
  - for host to create and remove LUN entry for Proxy Token

ASC/ASCQ Summary

ASC	ASCQ	Name	Function
20h	01h	ACCESS DENIED - INITIATOR PENDING-ENROLLED	An initiator in the pending-enrolled state sends a restricted command to a logical unit accessible under the enrolled AccessID
20h	02h	ACCESS DENIED - NO ACCESS RIGHTS	An initiator in the not-enrolled state sends an ACCESS ID ENROLL service action and the given AccessID has no access rights in the ACL
20h	03h	ACCESS DENIED - INVALID MGMT ID KEY	The Management Identifier Key value does not match the value maintained by the access controls coordinator
20h	04h	ACCESS DENIED - ENROLLMENT CONFLICT	An initiator in the enrolled or pending-enrolled state issues the ACCESS ID ENROLL service action under a different AccessID
20h	05h	ACCESS DENIED - INVALID LU IDENTIFIER	The LUN or default LUN does not correspond to a logical unit
20h	06h	ACCESS DENIED - INVALID PROXY TOKEN	The Proxy Token is not valid; it does not correspond to a logical unit
20h	07h	ACCESS DENIED - ACL CONFLICT	The enrollment failed because an ACL conflict occurred.
55h	05h	INSUFFICIENT ACCESS CONTROL RESOURCES	The device server has exhausted its resources for access controls

Open Questions

- ???

Contacts

- **Details**: `ftp://ftp.t10.org/t10/document.99/99-245r8.pdf`
- **e-mail**: `hafner@almaden.ibm.com`
- **phone**: 408-927-1892
- **fax**: 408-927-4182