TCG Update on SEDs

TCG SWG update & DTA OSS

Michael Romeo

Sr. Software Developer

Bright Plaza Inc.

SIIS 1.06 Public Review

- Storage Interface Interactions specification
  - Mostly NVMe updates
  - SPC-4, SBC-3 now approved references
  - SPC-5, SBC-4 now references in development

Compliance Certification

- Full certification process
  - Improved and Expanded Test Cases
  - Certified Test Programs
  - Certified Test Houses
  - Requires Common Criteria crypto certification

Ongoing Updates

- Modernize Specifications (WIP)
  - Expand NVMe support
  - Update Enterprise Specification
  - Update Opallite Specification
  - Need to keep pace with industry
    - Process improvement
    - More timely delivery

Drive Trust Alliance OSS

- Sedutil OSS (GPL3+)
  - Supports OPAL (1 & 2) and Enterprise SSC
  - Attachment Support for SATA, USB and M.2 NVMe*
  - Focused on Single User/Small Office
  - Host management software and PBA
  - Customized solutions available

* Full support in Linux, limited support in Windows

Drive Trust Alliance OSS

- Host Program – sedutil-cli
  - Discovery
  - Query status
  - TakeOwnership
  - Configure Locking ranges and MBR shadow
  - Enable/Disable Locking and MBR shadow
  - Crypto Erase
  - PSID revert support

Drive Trust Alliance OSS

- Pre-Boot Authorization Images
  - Legacy BIOS and UEFI 64bit support
  - Loaded to shadow MBR with host software
  - Requests PassPhrase and unlocks drives

Drive Trust Alliance OSS

- Available on GitHub:
  - https://github.com/Drive-Trust-Alliance/sedutil
  - https://github.com/Drive-Trust-Alliance/sedutil/wiki/Executable-Distributions
- Custom OEM solutions available
  - GPL/Open Source licensing not required