TCG Storage Work Group Update

Chandra Nelologal
DMTS, Dell Technologies
Co-Chair, Storage Work Group, TCG
Agenda

• Introduction
• Learning Objectives
• Status Update of several documents
• Upcoming plans
• Other sessions
Introduction

• We represent the TCG (Trusted Computing Group)
  – TCG Covers many things security (Storage, TPM, Platform, PC Client, Server, DICE, etc.)
  – Trustedcomputinggroup.org

• Storage Work Group
  – Focuses on security features specific to storage devices and solutions
  – Data at rest security specifications (SSCs)
    • Enterprise, Opal, Ruby, Pyrite, KPIO
  – Storage Interface Interactions Specification (SIIS)
  – Feature sets, supplementals to SSCs, References, Test Documents
    • CNL, Configurable PINs, Block SID, etc.
Learning Objectives

• Get an overview of the current activities w.r.t. standards
• Get a preview of upcoming standards activities
• Security trends in storage
• Help plan for your security features and capabilities
  – For your organization’s products and solutions
• Welcome your participation and input
No active work currently

- Core Specification
- Enterprise SSC
- Ruby SSC
- Pyrite SSC
## Recent Work On Specifications/References

<table>
<thead>
<tr>
<th>Document</th>
<th>Status</th>
<th>Timeline</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Opal Feature Set: Configurable Locking for NVMe NS and SCSI LUNs - V1.02, R1.16</td>
<td>Published</td>
<td>Feb 2023</td>
<td>Opal SSC feature set: Defines relationships between locking objects and LBA ranges and NVME Namespaces and SCSI LUNs</td>
</tr>
<tr>
<td>SIIS - V1.11, R1.18</td>
<td>Published</td>
<td>April 2023</td>
<td>Most referred to for TCG Protocol Mapping and SAS/SATA/NVMe interfaces: User data removal methods</td>
</tr>
<tr>
<td>Opal Family Test Case Spec - V1.01 R1.10</td>
<td>Published</td>
<td>May 2023</td>
<td>Test Specification: Essentially updated to support Opal 2.02</td>
</tr>
<tr>
<td>Opal Feature set: C_PIN Enhancements - V1.00, R1.21</td>
<td>Published</td>
<td>May 2023</td>
<td>Opal SSC feature set: Enhances PIN Configurability and properties</td>
</tr>
<tr>
<td>Key Per I/O (KPIO) SSC - V1.0, R1.41</td>
<td>Published</td>
<td>Sep 2023</td>
<td>New Approach to D@RE with host managed media encryption keys</td>
</tr>
</tbody>
</table>

2023 has been a productive year for the Storage Work Group  
All Specifications and References focus on Data at Rest Encryption (D@RE) technologies
Recent Work On Specifications/References

<table>
<thead>
<tr>
<th>Document</th>
<th>Status</th>
<th>Timeline</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Opal Feature set: Additional Data Store Tables V1.01, R1.17</td>
<td>Public Review</td>
<td>July – Oct 2023</td>
<td>Opal SSC feature set: Defines data store table creation for multi-client like use cases</td>
</tr>
<tr>
<td>App Note: KPIO</td>
<td>Completed Public review</td>
<td>July – Aug 2023</td>
<td>Reference document/Implementation guide for KPIO SSC</td>
</tr>
<tr>
<td>Test Cases &amp; FAQ: KPIO</td>
<td>In Development</td>
<td>NA</td>
<td>Additional documents related to KPIO</td>
</tr>
<tr>
<td>Errata for Opal 2.02</td>
<td>In Development</td>
<td>NA</td>
<td>Clarifications and errata fixes</td>
</tr>
<tr>
<td>SIIS 1.12</td>
<td>In Development</td>
<td>NA</td>
<td>Fixes and Enhancements. Inclusion of Key Per I/O related changes</td>
</tr>
</tbody>
</table>

All Specifications and References focus on Data at Rest Encryption (D@RE) technologies
SIIS 1.11 – Main changes

• Added Support for NVDIMM-N and SD-Card interfaces
• More details on User Data Removal methods
• Support for zoned commands
  – SCSI
  – ATA
  – NVMe
• NVMe – Mapping of MI resets
C_PIN Enhancements

• C_PIN Enhancements Feature (optional feature)
  – Configurable C_PIN TryLimit per Authority
  – Configurable C_PIN Persistence per Authority
  – Min and Max PIN length

• C_PIN Forced PIN Change (optional feature)
  – When enabled, requires the Authority PIN change before the authentication
  – Forced PIN change by allowing only Set method on the PIN column and Random method
Additional Data Store Tables

• Mechanism to configure additional tables in the data store
  – Partition the data store
  – Enables additional use cases
Configurable Locking NS and SL

- NVMe Namespaces
  - Assign/Deassign and Set Methods
- SCSI LUNs
  - Assign/Deassign Methods

Figure 1 - Locking SP Modes (NVMe)

Figure 2 - Locking SP Modes (SCSI)
Monitoring

- SNIA Key Management
- OCP Security requirements
- SPDM Storage Binding
- Quantum Safe Readiness
BACKUP
Focus Areas

Which types of technologies are being addressed?

- Interfaces: NVMe, ATA, SCSI, eMMC, NVDIMM-N, SD Card
- Self-encrypting storage (Opal, Ruby, Pyrite, Enterprise, etc.)
- Self-Encrypting storage, with external key management (Key Per I/O, new)

What is their impact on the industry?

- Main Data at Rest technology used in the industry
  - Widely accepted and continues to evolve
- Provide a standard way for managing SEDs
- Standards compliant and Certified SEDs are mandated by some governments and companies
- TCG work is being referenced by international standards (ISO, IEEE, NVMe, INCITS, etc.)
KPIO – Refer to focused session
Configurable Locking Objects

- Global Range Locking object
  - Any namespace or LUN that is not associated with below
- Namespace Global Range Locking object
  - First Locking object to be associated with a Namespace/LUN
- Namespace Non-Global Range Locking object
  - Locking object associated with an LBA range within a namespace/LUN
SUM and CNL

- Add parameter to Assign to indicate caller wants to associate Namespace with an available SUM range
- Mandate:
  - Assign to SUM Range results in erase of data
  - Deassign from SUM Range results in erase of data
    - KeepNamespaceGlobalRangeKey = True results in failure of Deassign method

For SUM ranges: NS1 Key is always erased and new key ownership is transferred from Range1 to Global Range, data is always erased when transitioning from SUM range.