Q. What is the Storage Work Group?
A. The Storage Work Group is an entity within the Trusted Computing Group. It consists of TCG member companies with interests in the implementation of the Trusted Computing Group’s specifications for storage devices. For more information on the Storage Work Group, please refer to www.trustedcomputinggroup.org.

Q. What is the purpose of the Storage Work Group?
A. The Storage Work Group builds upon existing TCG philosophy in the development of specifications that provide a comprehensive architecture for storage devices. The Storage Work Group’s objective is to define specifications and accompanying documents for building and managing storage devices that enforce policy controls as set by hosts across a wide range of storage transport command protocols.

Q. How is the Storage Work Group organized?
A. The Storage Work Group operates under the auspices of the TCG. Membership in the Storage Work Group is determined by TCG bylaws and is open to all TCG members.

Q. Who is participating in the Storage Work Group?
A. Participation in the Storage Work Group includes storage device manufacturers, storage subsystem manufacturers, software vendors, and designers of custom, highly integrated components. Storage and security management and storage integration vendors also participate. A complete list of current TCG members is available at www.trustedcomputinggroup.org.

Q. What is the output of this Work Group?
A. The Storage Work Group deliverables include specifications that define security functionality requirements for storage devices and managing hosts; test cases and certification process documents; and informative supporting documents.

Q. What is the Core Specification?
A. The Core Specification, officially known as TCG Storage Architecture Core Specification, developed by the Storage Work Group provides a comprehensive definition of TCG-related functions for a TCG storage device.

Q. What is a Security Subsystem Class (SSC)?
A. The Core Specification can be further broken down in multiple subsets of functionality called Security Subsystem Classes (SSCs). SSCs explicitly define the minimum acceptable Core Specification capabilities of a storage device in a specific “class” and potentially expand functionality beyond what is defined in the Core Specification.
Q. What is the Opal SSC?
A. The Opal SSC specification is predicated on ease of implementation and integration. This SSC defines the functionality for implementing the Core Specification on storage devices.

Q. What is the audience for this specification?
A. The target audience includes system integrators, security software vendors, test suites vendors, OEMs, and storage device manufacturers.

Q. What features are specified by the Opal SSC specification?
A. The Opal SSC provides data-at-rest protection of user data via data encryption and access controls, secure boot capability (pre-boot authentication), and fast repurposing of the storage device.

Q. How is user data protected?
A. The Opal SSC specifies multiple storage ranges with each having its own authentication and encryption key. The range start, range length, read/write locks as well as the user read/write access control for each range are configurable.

Q. Why do we need Opal SSC devices?
A. Opal SSC specifies a hardware based data encryption solution to the problem of data breach caused by lost or stolen storage devices.

Q. Do Opal SSC devices require a TPM?
A. No, Opal SSC storage devices do not require a TPM. For additional protection, integrating these storage devices in systems with an activated TPM is recommended.

Q. What's new in Opal SSC v2.00 Specification?
A. Opal SSC v2.00 includes the following new and enhanced capabilities:

- **LBA Range Alignment:** Configuration options for LBA range alignment in storage devices with more than 1 logical block per physical block on the media and where the first logical block may not line up exactly with the beginning of a physical block.

- **Byte Table Access Granularity:** Writing to byte tables, such as the DataStore table and the MBR table in the Locking SP, can now be required to be done in blocks of granularity larger than a byte.

- **Admin Authorities:** The minimum supported number of Admin Authorities in the Locking SP has been increased to 4. New Admin Authorities (a minimum of 1) have been added to the Admin SP.

- **User Authorities:** The minimum supported number of User Authorities has been increased to 8. A configuration option for disallowing User Authorities to change their C_PIN values has been added.

- **LBA Ranges:** The minimum number of supported LBA ranges has been increased to 8.

- **Methods and Commands:** More methods and commands are now Mandatory in Opal SSC v2.00, including the Protocol Stack Reset and TPer Reset commands, and the Authenticate, Random and Revert methods (on both the Locking SP and the Admin SP).

- **Columns and Tables:** More columns of certain tables are now Mandatory in Opal SSC v2.00. This includes the CommonName column in the Authority and Locking tables of the Locking SP, and the
GUDID column in the TPerInfo table of the Admin SP. A new SecretProtect table has been added to the Locking SP.

- Default SID PIN Value: The initial value of C_PIN_SID may be Vendor Unique (instead of being set to C_PIN_MSID).

- DataStore Table: The minimum size of the DataStore table has been increased to 10MB (from 1KB). The Additional DataStore Tables Feature Set has been made Mandatory.

**Q. Is the Opal SSC v2.00 a superset of the Opal SSC v1.00?**

**A.** Yes. The Opal SSC v2.00 specification extends the existing features of Opal SSC v1.00 and adds additional features.

**Q. Is the Opal SSC v2.00 specification backwards compatible with the previous Opal SSC v1.00 specification?**

**A.** No. The Opal SSC v2.00 specification itself is not backwards compatible. However, Opal SSC v2.00 allows a storage device vendor to implement a device based on Opal SSC v2.00 in a way that is backwards compatible with Opal SSC v1.00.

**Q. Why was the backwards incompatibility introduced in Opal SSC v2.00?**

**A.** The Opal SSC v2.00 specification was extended to allow storage devices with physical block size restrictions to be supported.

**Q. How can I tell if a storage device supports both versions of the Opal specifications?**

**A.** The storage device will report the Opal SSC Feature Descriptors for both specifications.

**Q. What are the benefits of the Opal SSC v2.00 specification?**

**A.** Opal SSC v2.00 will accommodate a wider range of storage devices. The addition of new features allows delivery of a richer set of solutions around self-encrypting drives.

**Q. What is a Feature Set?**

**A.** A Feature Set defines additional functionality that extends an SSC.

**Q. Are there any Mandatory Feature Sets for Opal SSC v2.00?**

**A.** Yes. The Additional DataStore Tables Feature Set is Mandatory for Opal SSC v2.00.

**Q. Can Opal SSC v2.00 storage devices work with host software designed for Opal SSC v1.00?**

**A.** Yes, if the storage device was implemented to support both the Opal SSC v1.00 and Opal SSC v2.00 specifications.

**Q. How does a storage device vendor implement a device based on Opal SSC v2.00 so that it is compatible with Opal SSC v1.00?**

**A.** An Opal SSC v2.00 implementation is compatible with Opal SSC v1.00 only if the geometry reported by the Geometry Reporting Feature does not specify any alignment restrictions; the TPer does not specify any granularity restrictions for byte tables; and the “Initial C_PIN_SID PIN Indicator” and “Behavior of C_PIN_SID PIN upon TPer Revert” fields are both 0x00 in the Opal SSC V2.00 Level 0 Feature Descriptor. The storage device will report the Opal SSC Feature Descriptors for both specifications.

**Q. What’s new in Opal SSC v2.01 Specification?**

**A.** The Opal SSC v2.01 specification adds one new mandatory Feature Set and introduces some editorial

Q. Are there any additional Mandatory Feature Sets for Opal SSC v2.01?

A. Yes. The TCG Storage Opal SSC Feature Set: PSID was added and is now Mandatory for Opal SSC v2.01.

Q. What's new in Opal SSC v2.02 specification?

A. The Opal SSC v2.02 specification includes the following new and enhanced capabilities (refer to Table 1 for details):

- Adds one new mandatory Feature Set.
- Selectable data removal mechanism added.
- Methods and Commands: Rules of side effect of Revert and RevertSP methods have been updated due to the addition of user data removal.
- Optional support for Hardware Reset as an option for LockOnReset and DoneOnReset added.
- Support for the manufactured-Inactive state is now mandatory.
- The specification now references the updated TCG Storage Interface Interactions Specification, Version 1.09 and TCG Storage Feature Set Block SID Authentication, Version 1.00.

Q. Are there any additional Mandatory Feature Sets for Opal SSC v2.02?

A. Yes. The TCG Storage Feature Set: Block SID Authentication was added and is now Mandatory for Opal SSC v2.02.

Table 1 Opal 2.02 Changes from Opal 2.01

<table>
<thead>
<tr>
<th>Opal 2.02 Section</th>
<th>Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.10</td>
<td>Added &quot;Block SID Authentication Feature Set&quot; to list of Mandatory Feature Sets</td>
</tr>
<tr>
<td>3.1.1</td>
<td>Added the optional Level 0 Discovery descriptor response: &quot;Supported Data Removal Mechanism Feature Descriptor&quot;</td>
</tr>
<tr>
<td>3.1.1.3</td>
<td>Added new fields: MBR Shadowing Not Supported -&gt; Shall be 0 to indicate feature is supported HW Reset for LOR/DOR Supported -&gt; VU field Changed Version field: &quot;0x1 or any version that supports the defined features in this SSC&quot; -&gt; &quot;0x3 or any version that supports the defined features in this SSC&quot;</td>
</tr>
<tr>
<td>3.1.1.5</td>
<td>Changed name of Version field in byte 2 to &quot;Feature Descriptor Version Number&quot; Changed name of Reserved field in byte 2 to &quot;SSC Minor Version Number&quot; Version description removed and replaced with: &quot;Feature Descriptor Version Number = 0x2 or any version that supports the defined features in this SSC&quot; New definition added: SSC Minor Version Number = As specified in Table 8 Changed &quot;Number of ComIDs&quot; field: &quot;0x0001 (minimum value)&quot; -&gt; &quot;0x0001 or larger&quot;</td>
</tr>
<tr>
<td><strong>3.1.1.6</strong></td>
<td>Added new level 0 feature descriptor to section 3.1.1.6: Supported Data Removal Mechanism Feature (Feature Code = 0x0404)</td>
</tr>
<tr>
<td>4.2.1.3</td>
<td>New entry to AdminSP Table Table:</td>
</tr>
<tr>
<td>4.2.1.5</td>
<td>New rows added to AdminSP AccessControl Table Preconfiguration:</td>
</tr>
<tr>
<td>4.2.1.6</td>
<td>New rows added to AdminSP ACE Table Preconfiguration:</td>
</tr>
<tr>
<td>4.2.1.8</td>
<td>Updated cell shade of C_PIN_Admin1 and C_PIN_AdminXX PIN column No functional change since ACE and AccessControl table did not change</td>
</tr>
<tr>
<td>4.2.5</td>
<td>New section added for Opal Column: data_removal_mechanism</td>
</tr>
<tr>
<td>4.2.6</td>
<td>New section added for Opal Data Structure: DataRemovalMechanism</td>
</tr>
<tr>
<td>4.2.7</td>
<td>New section added for Opal Object Table: DataRemovalMechanism</td>
</tr>
</tbody>
</table>

**Table 8 - SSC Minor Versions for valid values for SSC Minor Version Number**

<table>
<thead>
<tr>
<th>Version</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1.1.6</td>
<td>Added new level 0 feature descriptor to section 3.1.1.6: Supported Data Removal Mechanism Feature (Feature Code = 0x0404)</td>
</tr>
<tr>
<td>4.2.1.3</td>
<td>New entry to AdminSP Table Table:</td>
</tr>
<tr>
<td>4.2.1.5</td>
<td>New rows added to AdminSP AccessControl Table Preconfiguration:</td>
</tr>
<tr>
<td>4.2.1.6</td>
<td>New rows added to AdminSP ACE Table Preconfiguration:</td>
</tr>
<tr>
<td>4.2.1.8</td>
<td>Updated cell shade of C_PIN_Admin1 and C_PIN_AdminXX PIN column No functional change since ACE and AccessControl table did not change</td>
</tr>
<tr>
<td>4.2.5</td>
<td>New section added for Opal Column: data_removal_mechanism</td>
</tr>
<tr>
<td>4.2.6</td>
<td>New section added for Opal Data Structure: DataRemovalMechanism</td>
</tr>
<tr>
<td>4.2.7</td>
<td>New section added for Opal Object Table: DataRemovalMechanism</td>
</tr>
</tbody>
</table>

**Changed equation from:**

\[
\text{StartAlignment} = \left( \text{RangeStart} \mod \text{AlignmentGranularity} \right) - \text{LowestAlignedLBA}
\]

**To:**

\[
\text{StartAlignment} = \left( \text{RangeStart} - \text{LowestAlignedLBA} \right) \mod \text{AlignmentGranularity}
\]
<table>
<thead>
<tr>
<th>Section</th>
<th>Changes</th>
</tr>
</thead>
</table>
| 4.3.5.2.1.1 | Changed equation from:  
StartAlignment = (RangeStart modulo AlignmentGranularity) - LowestAlignedLBA  
To:  
StartAlignment = (RangeStart - LowestAlignedLBA) modulo AlignmentGranularity |
| 4.3.5.2.1.2 | Changed equation from:  
If RangeStart is zero, then  
LengthAlignment = (RangeLength modulo AlignmentGranularity) - LowestAlignedLBA  
To:  
If RangeStart is zero, then  
LengthAlignment = (RangeLength - LowestAlignedLBA) modulo AlignmentGranularity |
| 4.3.5.2.2 | New optional values for LockOnReset  
Additionally, the TPer MAY support the following LockOnReset column values:  
a) \{0, 1\} (i.e. Power Cycle and Hardware Reset); and  
b) \{0, 1, 3\} (i.e. Power Cycle, Hardware Reset and Programmatic). |
| 4.3.5.3.1 | New optional values for DoneOnReset  
Additionally, the TPer MAY support the following DoneOnReset column values:  
a) \{0, 1\} (i.e. Power Cycle and Hardware Reset); and  
b) \{0, 1, 3\} (i.e. Power Cycle, Hardware Reset and Programmatic). |
| 4.3.7 | Removed the following text from this section:  
The SD SHALL terminate with a "Data Protection Error" as defined in [4]:  
- Read commands that address consecutive LBAs in one or more locked LBA ranges. Locked range is ReadLockEnabled= True and ReadLocked= True.  
- Write commands that address consecutive LBAs in one or more LBA ranges for which WriteLockEnabled= True and WriteLocked= True. |
| 5.1.2.2 | New text added to section:  
Upon successful invocation of the Revert method, the following changes SHALL be made:  
- If the Locking SP is in the "Manufactured-Inactive" life cycle state, then successful invocation of the Revert method on the Locking SP or Admin SP SHALL cause user data removal as defined by the ActiveDataRemovalMechanism (see Table 34) and cause the media encryption keys to be eradicated, which has the side effect of securely erasing all data in the User LBA portion of the SD.  
- If the Locking SP is in the "Manufactured-Inactive" life cycle state, then successful invocation of the Revert method on the Locking SP SHALL NOT cause user data removal in the SD.  
Interactions with interface commands during the processing of the Revert method are defined in [4].  
If any TCG reset occurs prior to completing user data removal and the eradication of all media encryption keys in the SD, then the Revert operation SHALL be aborted and the Locking SP SHALL NOT revert to its Original Factory State.  
**Start of Informative Comment**  
If any TCG reset occurs during the processing of the Revert method, the result of user data removal is undefined and the TPer does not erase personalization of the Locking SP. For example, the PIN column value for each row in C_PIN table is unchanged.  
**End of Informative Comment**
### 5.1.2.3 New section added

**5.1.2.3 Interrupted Revert**

The Revert method and complete implementation of necessary background operations MAY be aborted due to any reset condition, including power loss.

When interrupted, the Data Removal Operation Interrupted bit SHALL be set to one in the Level 0 Discovery – Supported Data Removal Mechanism feature descriptor appropriately as defined in section 3.1.1.6.2.

Further, the return status value of the `Revert` method does not mean that all necessary operations, such as the background deallocate, or trim, or un-map are complete.

### 5.1.3.2 Added detail about `DataRemovalMechanism` table:

<table>
<thead>
<tr>
<th>Added detail about <code>DataRemovalMechanism</code> table:</th>
</tr>
</thead>
<tbody>
<tr>
<td>When this parameter is present and set to True, the TPer SHALL NOT erase data associated with the Global Locking Range after the Locking SP transitions to the &quot;Manufactured-Inactive&quot; state even if the valid value is set to the ActiveDataRemovalMechanism parameter in DataRemovalMechanism table.</td>
</tr>
</tbody>
</table>

Split paragraph into positive and negative case:

If the Global Range is either Read Unlocked or Write Unlocked at the time of invocation of `RevertSP`, then the TPer SHALL comply with the request to keep the user data associated with the Global locking range and the Global Range's media encryption key.

If the Global Range is Read Locked and Write Locked then invocation of the `RevertSP` method with the `KeepGlobalRangeKey` parameter set to True SHALL fail with status FAIL, and the SP SHALL NOT change life cycle states.

### 5.1.3.3 Added text:

Upon successful invocation of the `RevertSP` method, the following changes SHALL be made:

- If the `KeepGlobalRangeKey` parameter is not present or set to False, then successful invocation of the `RevertSP` method on the Locking SP or Admin SP SHALL cause user data removal as defined by the ActiveDataRemovalMechanism (see Table 34) and cause the media encryption keys to be eradicated, which has the side effect of securely erasing all data in the User LBA portion of the SD.

- If the `KeepGlobalRangeKey` parameter is set to True, then successful invocation of the `RevertSP` method on the Locking SP SHALL cause user data removal in the SD all media encryption keys to be eradicated except for the Global Range's media encryption key (K_AES_{(128,256)}_GlobalRange_Key).

Interactions with interface commands during the processing of the `RevertSP` method are defined in [4].

If any TCG reset occurs prior to completing user data removal and the eradication of media encryption keys in the SD, then the operation SHALL be aborted and the Locking SP SHALL NOT revert to its Original Factory State.

### 5.1.3.4 New section

**5.1.3.4 Interrupted RevertSP**

The `RevertSP` method and complete implementation of the necessary background operations MAY be aborted due to any reset condition, including power loss.

When interrupted, the Data Removal Operation Interrupted bit SHALL be set to one in the Level 0 Discovery – Supported Data Removal Mechanism feature descriptor appropriately as defined in section 3.1.1.6.2.

Further, the return status value of the `RevertSP` method does not mean that all necessary operations such as the data removal operation are complete.
5.2.2 Updated “Life Cycle State Diagram for Manufactured SPs” diagram. Added new arrow from Manufactured state to Manufactured state:

![Life Cycle State Diagram](image)

**Changed:**

If the Locking SP is a Manufactured SP, its Original Factory State SHALL be Manufactured-Inactive or Manufactured.

If the Locking SP is a Manufactured SP, support of the Manufactured state is mandatory and support of the Manufactured-Inactive state is optional for the Locking SP.

**To:**

If the Locking SP is a Manufactured SP, its Original Factory State SHALL be Manufactured-Inactive. Support for Locking SP states of Manufactured and Manufactured-Inactive are mandatory.