



Storage Work Group Pyrite Security Subsystem Class (SSC) Specification FAQ November 2018

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, was developed by the Storage Work Group and 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 Pyrite SSC?

A. The Pyrite 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 Pyrite SSC specification?

A. The Pyrite SSC specification provides data-at-rest protection of user data via access controls over the storage interface and optional secure boot capability (pre-boot authentication).

Q. How is user data protected?

A. The Pyrite SSC specification specifies authentication requirements to unlock access to user data.

Q. Why do we need Pyrite SSC devices?

A. The Pyrite SSC specification specifies access control over user data without specifying requirements for encryption, in order to meet a wider range of use cases and market requirements while supporting the same command protocol as Opal SSC, Opalite SSC, and Ruby SSC specifications.

Q. Do Pyrite SSC devices require a TPM?

A. No, Pyrite 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 features does the Pyrite SSC specification support?

- A. The Pyrite SSC specification includes the following capabilities:
- Global Range: Specifies locking of a single range of LBAs that encompasses the entire user data space on the storage device.
 - Admin Authorities: Specifies support for 1 Admin authority.
 - User Authorities: Specifies support for 2 User authorities.
 - DataStore table: Specifies DataStore table size of 128 KB.
 - Optional MBR Shadowing: Support for the MBR Shadowing feature is Optional in the Pyrite SSC specification.

Q. Does the Pyrite SSC specification specify encryption of user data?

A. No, the Pyrite SSC specification does not specify encryption of user data.

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 the Pyrite SSC specification?

A. Yes, the Block SID Authentication Feature Set is Mandatory for the Pyrite SSC specification.

Q. Since the Pyrite SSC is a member of the Opal family, can other Opal family storage devices work with host software designed for the Pyrite SSC specification?

A. Yes, the Pyrite SSC specification has protocol level compatibility with the Opal family as they share a common Architecture Core specification.

Q. What's new in the Pyrite SSC v2.00 specification?

- A. The Pyrite SSC v2.00 specification includes the following new and enhanced capabilities:
- Mandatory Feature Set: PSID Feature Set has been added.
 - 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. KeepData parameter has been added to RevertSP method.



Q. Is the Pyrite SSC v2.00 specification backward compatible with Pyrite SSC v1.00?

A. No, the Pyrite SSC v2.00 specification itself is not backwards compatible. For example, Revert and RevertSP method behavior may be different between Pyrite SSC v1.00 and v2.00 from a host perspective. However, the Pyrite SSC v2.00 specification allows a storage device vendor to implement a device based on the Pyrite SSC v1.00 specification with minor modifications.

Q. Why was the backwards incompatibility introduced in the Pyrite SSC v2.00 specification?

A. The Pyrite SSC v2.00 specification incorporates a Data Removal feature so that the Pyrite SSC v2.00 specification can be more compatible with other Opal family SSCs. More specifically, the Revert and RevertSP methods defined in the Pyrite SSC v1.00 specification do not clearly mandate user data removal. The Revert and RevertSP methods defined in the Pyrite SSC v2.00 specification mandate user data removal in order to enhance security.

Q. How can I tell which version of the Pyrite specification a storage device supports?

A. The storage device will report a different Pyrite SSC Feature Descriptors (e.g. Feature Code) in Level 0 Discovery.

Q. What are the benefits of the Pyrite SSC v2.00 specification over 1.0?

A. The Pyrite SSC v2.00 specification was extended to allow storage devices with Data Removal feature to be supported so that it becomes compatible with other Opal family SSCs, and achieves feature parity with ATA Security. The Data Removal feature supports user data removal without requiring encryption.

Contact: press@trustedcomputinggroup.org.