Trusted Computing Group Storage Work Group

Pyrite Security Subsystem Class (SSC) Specification FAQ

August 2015

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 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?

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

Q. Why do we need Pyrite SSC devices?

A. Pyrite SSC 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 and Opalite SSC.

Q. Do Opalite SSC devices require a TPM?

A. No. Opalite SSC storage devices do not require a TPM. For additional protection, integrating these storage devices in systems with activated TPM is recommended.

Q. What is Pyrite SSC’s relationship with Opalite SSC?

A. Pyrite SSC is a subset of Opalite SSC.

Q. What features does Pyrite SSC support?

A. Pyrite SSC 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 Pyrite SSC. MBR Shadowing is Mandatory in Opalite SSC.

Q. Does Pyrite SSC specify encryption of user data?

A. Unlike Opalite SSC, Pyrite SSC 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 Pyrite SSC?

A. Yes. The Block SID Authentication Feature Set is Mandatory for Pyrite SSC.

Q. Since Pyrite SSC is a subset of Opalite SSC, can Opalite SSC storage devices work with host software designed for Pyrite SSC?

A. Yes. Some capabilities operate differently due to media encryption (as specified in Opalite SSC), or lack thereof (as specified in Pyrite SSC). For example, the Revert method in Pyrite SSC does not specify a means of media sanitization. Revert in Opalite SSC where the Locking SP was Activated results in a cryptographic erase of all user data.

Contact: **Anne Price**

+1 (602)840-6495

press@trustedcomputinggroup.org