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

Q. What is the Storage Work Group?

A. The Storage Work Group is an organization within the Trusted Computing Group. It consists of TCG member companies with interests in the implementation of the Trusted Computing Group's methodologies for storage. For more information on the Storage Work Group, please see the documents at **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 TCG Ruby SSC?

A. The Ruby SSC specification is predicated on ease of implementation and integration. This SSC defines the functionality for implementing the Core Specification on storage devices commonly deployed within, but not limited to, Data Center/Bulk Data/Enterprise class systems.

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. Do Ruby SSC devices require a TPM?

A. No, Ruby SSC storage devices do not require a TPM. As is true with all Trusted Computing Group specifications, the specifications do not specifically provide DRM capabilities or software and do not "lock" a user to a specific software or platform, nor are they intended to reduce a user's access to his or her own content or applications. For additional protection, integrating these storage devices in systems with an activated TPM is recommended.

Q. What features does the Ruby SSC specification support?

A. The Ruby 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). This SSC is part of the Opal family specifications and includes the following features:

- 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 Ruby SSC specification.
- Optional support for additional locking ranges.

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

A. Yes, the Ruby SSC specification requires implementation of Full Disk Encryption for all host accessible user data stored on media.

Q. Are there any Mandatory Feature Sets for the Ruby SSC specification?

A. Yes, the Block SID Authentication Feature Set and the PSID Feature Set are Mandatory for the Ruby SSC specification.

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

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

Contact: press@trustedcomputinggroup.org.