Trusted Computing Group Storage Work Group

TCG Storage Architecture Core Specification FAQ

August 2015

Q. What is the TCG Storage Architecture Core Specification?

A. The TCG Storage Workgroup has developed the TCG Storage Core Architecture Specification Version 2.01, Revision 1.00, which describes in detail how to implement and utilize trust and security services on storage devices. This is an update to the TCG Storage Core Architecture Specification Version 2.00 Revision 2.00 that was published in November 2011.

Q. Who would use the Storage Specification?

A. There are two primary audiences for this Specification:

- For storage device manufacturers, TCG's Specification provides the architecture for how to implement trust and security services on storage devices.
- For platform-based application developers (ISVs – independent software vendors), the Specification describes the interface to trust and security services on storage devices, so that the application can take advantage of such services.

Of course, the ultimate benefactors of the Storage Specification are the end-users who purchase and take advantage of the security-enhanced applications that will result from using the Specification.

Q. Have you taken into account existing standards such as those for SCSI, ATA or NVM Express? How are you working with other standards bodies?

A. SCSI (T10) and ATA (T13) are ANSI/INCITS standards committees that input their standards to ISO and provide the interface standards for a great variety of storage devices, including USB-attached storage (i.e., SCSI command set). After interaction with TCG, T10 and T13 both have defined a Trusted Send/Security Protocol Out and Trusted Receive/Security Protocol In command set, which have subsequently been dually standardized. NVM Express has adopted a similar command set, Security Send and Security Receive.

These are the "container" commands for specific "payload" security commands. The TCG Storage Specification provides the "payload" definition for the specific Protocol ID = TCG. Other Protocol IDs can be assigned to other protocol suites, as needed.

Additionally, the Storage Specification reference adopts other trust and security standards, as appropriate (e.g., for encryption).

Q. Is the TCG the only standards group working on security for storage?

A. No. The necessity for secure and trusted storage has been realized by a number of storage related standards groups, including: SNIA, IEEE P1667, IEEE P1619, U3, OASIS, IETF and others. Throughout the several-year work effort of the TCG Storage Workgroup, the objective has been to develop a comprehensive and flexible trust architecture that could be applied to a variety of storage environments and requirements, such as those being contemplated by the referenced groups. The work of the TCG Storage Workgroup is unique and complementary to these other groups.

Q. What does this Storage Specification enable?

A. The Specification enables platform-based applications to take advantage of trust and security services provided by "trusted" storage devices.

Q. What are examples of trust and security services detailed in the Storage Specification?

A. The Specification enables applications to take advantage of a number of trust and security services on a storage device, including:

- Cryptography
- Random number generation (RNG)
- Secure storage

Q. Will products created using today's Storage Specification work with those based on later versions?

A. Yes Any enhancements and additions should be upward compatible or require minimal changes.

Q. Will products based on the Storage Specification work in today's PC architectures?

A. Yes. The Storage Specification targets applications running on either PC or server platforms and therefore takes advantage of and is compatible with PC and server architectures.

Q. What change of behavior is required from IT managers to use products based on the Storage Specification?

A. Traditionally, storage devices have been viewed as "simply" storage. However, storage devices can have powerful computing systems on board and lots of available memory, all protected behind a tightly closed and access-controlled environment, largely immune to the vulnerabilities of the operating system-based platform itself (e.g., viruses). And, the data is on the storage device. Why not put the security functions related to data protection directly on the device housing the data?

TCG and its members believe that IT managers will appreciate the advantages of pairing security and data storage in the same device.

Q. Do you expect to see trusted storage devices in consumer products? If so, which ones and when?

A. As noted, all the major hard drive manufacturers have actively participated in developing this Specification, as well as flash, tape, and optical manufacturers. TCG develops specifications, not products, so we cannot speculate on product timelines, but the level of engagement from the storage device manufacturers suggests Storage Specification-based products will appear in the near future.

Q. Does implementing this Storage Specification cost storage device makers more? If so, how much?

A. Yes. The implied firmware and hardware enhancements needed to support the Specification cost money and development resources. But, the storage device industry has a tradition of efficient and cost-effective development, as well as an "economy of scale" across such large product volumes.

Q. Does implementing this Storage Specification require any new or different parts for storage devices? If so, who is providing those and when will they be available?

A. Yes. The internal computing environment of a storage device must be enhanced to support the Specification. The storage device manufacturers themselves typically develop those core components themselves. TCG cannot speculate on availability, except to note that the storage device industry had been aggressively cooperating on the development of the Specification.

Q. How will PC makers and users know that storage devices based on the Storage Specification meet all of its requirements? Are you planning a certification program?

A. The TCG Storage Workgroup is working on compliance requirements as a follow-on effort.

Q. What are the benefits of secure storage?

A. "Storage" is where sensitive data spends most of its productive life. Sensitive data is vital to the competitiveness and viability of modern business. Storage must be secured. Why not put the security function on the same device that stores the sensitive data?

Q. Will secure storage devices require a separate TPM?

A. The requirements derived from the Storage Workgroup use cases do not mandate a Trusted Platform Module (TPM) for storage devices.

Q. Which companies are participating in the Storage Specification effort?

A. More than 60 TCG members have registered for participation in the development of the Storage Architecture Core Specification. Not only all major hard drive vendors, but flash, tape, and optical storage vendors are currently participating or have participated in the development and the Storage specifications. We also have participation from storage and security management and storage integration vendors. A complete list of TCG members is online at www.trustedcomputinggroup.org.

Q. Could trusted storage be embedded into other devices such as mobile systems or embedded systems?

A. Yes. For example, the TCG trusted protocols operate at the SCSI and ATA interface level for storage devices supporting those standards, regardless of how those devices are further embedded in larger systems.

Q. What are some potential applications for trusted storage?

A. Every application that depends on the integrity, trustworthiness, and security of relevant data will critically benefit from the TCG Storage Architecture Core Specification. The published storage use case white paper implicates a number of such applications. That document can be seen at www.trustedcomputinggroup.org.

Q. Is the Storage Specification targeted for content protection?

A. The Specification does not define a complete, full-life-cycle content protection scheme. However, the Specification does provide a number of security "building blocks" that could be used by developers of content protection schemes.

Q. How does trusted storage work, exactly?

A. Once the trust and security functions from the Specification are implemented in firmware and hardware on the storage device, then platform-based applications utilize this function through the SCSI/ATA Trusted Send/Receive command interface, under versatile access control.

Q. Why is the storage subsystem appropriate for security? Why not put security further out, for example, in the SAN or the RAID device?

A. Storage is where the data resides! Plus, storage devices contain powerful computing subsystems and lots of available memory, as well as being “closed” to vulnerabilities that plague the operating system-based platform. SAN, RAID, and other complex storage device manufacturers are reacting favorably to such trust and security functions being provided by the constituent storage devices; e.g., scale and extensibility, shorter path lengths, risk mitigation, etc. Also, putting security on the storage device itself simplifies data shredding, device repurposing and device replacement/cloning.

Q. Is TCG going to address security issues for data centers as well as notebooks?

A. Yes. The Specification applies to ALL storage devices, both client (PC) and server. The capabilities defined in the Specification will appear in all storage, equally satisfying requirements that are specific to servers and data centers.

Q. Does the Storage Specification address flash drives and other portable storage devices?

A. Yes. The Specification applies to ALL storage devices and we have had participation in development of the Specification from all storage device types. For more information on the TCG’s Storage Work group and its efforts, go to www.trustedcomputinggroup.org.

Q: How does the TCG Storage Core Architecture Specification Version 2.00 Revision 1.00 differ from Version 1.0 Revision 0.9 - draft?

A. The TCG Storage Work Group released Version 1.0 Revision 0.9 - draft as a draft version for wider industry review, before publishing a final version of the Core Architecture Specification. As the Storage Work Group developed the Enterprise SSC, Opal SSC, and Optical SSC specifications, and as the member companies worked on implementing SSC-compliant products, the Work Group made many improvements in the Core Architecture Specification to remove specification ambiguities, add necessary clarifications, and allow for simpler implementation. Version 2.00 Revision 1.00 is the culmination of these efforts.

Q: How does the TCG Storage Core Architecture Specification Version 2.00 Revision 2.00 differ from Version 2.00 Revision 1.00?

A. The TCG Storage Core Architecture Specification Version 2.00 Revision 2.00 is an errata revision that contains numerous editorial modifications and clarifications based on review of the document and development of the TCG Storage Security Subsystem Class: Opal. This revision does not include any additional features.

How does the TCG Storage Core Architecture Specification Version 2.01 Revision 1.00 differ from Version 2.00 Revision 2.00?

The TCG Storage Core Architecture Specification Version 2.01 Revision 1.00 fixes an elevation of privileges issue by removing the section that defined behavior for authority authentication within transactions. Additionally, the specification now references the updated TCG Storage Interface Interactions Specification, Version 1.04, and fixes (minor) editorial issues.

Contact: **Anne Price**

+1 (602)840-6495

press@trustedcomputinggroup.org