Trusted Computing Group Storage Use Cases
FAQs

Q. Why is TCG publishing these storage use cases?
A. The Storage Work Group (WG) of Trusted Computing Group (TCG) is working on a detailed specification for extending trust and security to storage devices. That specification is expected to be publicly available in the first half of 2006. In the meantime, these use cases are intended to show to the storage community the scope of the scenarios that will be solved by the specification.

Q. What scenarios are covered by these use cases?
A. The seven use cases in the white paper were chosen from a much larger set of use cases that were analyzed by the Storage WG and which contributed to the specification under development. These use cases are both representative and illustrative and include:

- Enrollment and connection: trusted relationship between the storage device and the host
- Protected storage: for storing sensitive data
- Locking and encryption: mating a storage device and host; encrypting stored data at rest
- Logging: for forensic purposes
- Cryptographic services: supporting a variety of security services
- Authorizing storage device feature sets to hosts: for trusted and exclusive use
- Secure download of firmware: trusting firmware upgrades

Q. What is the relevance of these use cases from TCG?
A. The TCG initially focused on creating a trusted host platform. Recent work has shifted to extending that trust boundary to peripheral devices, such as mobile devices and storage devices.

Q. Who do these use cases affect?
A. Any vendor creating storage solutions should review these use cases and should subsequently implement the resulting specification. In the storage world, attention to security has traditionally not been a top priority. However, the protection of corporate data is vital to the competitiveness of any business.

Q. Why are these use cases necessary?
A. These use cases were contributed and analyzed by the Storage WG, which has active membership from a cross-section of the storage and user community. Not only flash storage vendors but the major hard drive vendors are participating. These participants strongly agree that these use cases, drawn from the larger validated set, represent critical yet unsolved customer requirements.

Q. Why is a storage solution required?
A. What is a trusted platform without trusted storage? The trust boundary must be extended to peripheral devices that make up a multi-component trusted platform. A “chain is no stronger than its weakest link” is especially true of platform-attached storage.
Q. Do these storage use cases contemplate connected, peripheral and rack-based storage?
A. Yes. The specification will focus on each storage component, such as an individual hard drive or flash storage device, but networked or array-based storage will have the individual components managed by a trusted controller.

Q. Are there concerns with protocol or design requirements that should be considered?
A. The totality of use cases considered by the Storage WG have been carefully analyzed and the specification is being cautiously drafted through extensive telecons and face-to-face meetings. The collective technical expertise of the storage and security community is being leveraged.

Q. What is the trust model contemplated by these use cases?
A. The trust model had two basic elements:
   - a trusted host platform that interacts with a trusted storage device;
   - trusted storage device, with every access port and functionality under versatile authentication and access control.

Q. Are there certification requirements for storage products that will implement the specification?
A. TCG as a whole is studying the issue of conformance and compliance to TCG specifications. No certification methodologies have yet been finalized. The storage specifications will certainly be subject to any such certification.

Q. When does TCG anticipate delivering a storage specification? And, what is anticipated to be the goal of this specification?
A. The specification is expected to be publicly available in the first half of 2006. The goal of the specification is to extend the trust boundary from the trusted platform to storage devices.

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, etc. Throughout the several-year work effort of the TCG Storage WG, 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.

Q. What is the relationship of the TCG Storage WG specifications to the INCITS/ISO standards T10/SCSI and T13/ATA?
A. SCSI and ATA provide the interface standards for a great variety of storage devices, including USB-attached storage (i.e., SCSI command set). The TCG Board requested that T10 and T13 both define a Trusted Send (In) and Trusted Receive (Out) command set. Draft proposals for such extended commands have been under review for some time and voting is expected in the first quarter of 2006. The Trusted Send/Receive would provide the “container” commands and the TCG specification will provide the “payload” set of commands specific to Protocol ID = TCG. Other Protocol IDs can be assigned to other protocol suites, as needed.
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.

Q. Will secure storage devices require a separate TPM?
A. The requirements derived from the Storage WG use cases do not mandate a Trusted Platform Module (TPM) for storage devices. However, a "root of trust" for storage devices is required to extend the trust boundary of trusted platforms. This 'root of trust' is detailed in the specification and can be realized by a combination of hardware and firmware.

Q. When do you expect products to be available?
A. The specification is expected to be available in the first half of 2006. We cannot speculate on when related products will be available, but the mandate exists for storage device makers to respond quickly.

Q. Which companies are participating in the spec effort?
A. 39+ member companies of the 115+ TCG members have registered for participation in the development of the Storage WG specifications. Not only flash storage vendors but the major hard drive vendors are participating. We also have participation from storage management and storage integration vendors. A complete list of members is online at www.trustedcomputinggroup.org.

Q. How does trusted storage relate to other parts of the trusted enterprise?
A. The concept under detailed investigation in the TCG is the Multi-Component Trusted Platform (MCTP), including how the trust boundary is extended uniformly to encompass the MCTP. Trusted Storage plays a fundamental role in the MCTP.

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 across and 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 WG specifications. The published use case white paper implicates a number of such applications.

-- 30 --