Trusted Computing Group Storage Work Group
TCG Storage Protection Mechanisms for Secrets FAQ
March 2012

Q. What is defined in the TCG Storage Protection Mechanisms for Secrets specification?
A. This specification defines a mechanism by which a host can query a Storage Device to determine how critical security values (such as media encryption keys) are protected.

Q. What Storage Devices and versions report the values specified in the SecretProtect table?
A. Storage Devices supporting the Opal SSC version 2.0 revision 1.0 and later are required to report these values for identifying the mechanisms used to protect secrets, such as the media encryption key(s). Storage Devices supporting a version of Opal SSC prior to version 2.0 or any version of the Enterprise SSC can report these values, but are not required to do so by the specifications.

Q. What is the difference between the reported values?
A. If '0' is reported, the Storage Device uses a vendor unique scheme for protecting the secret, and the protection may be logical (such as an access control list) versus cryptographic. If '1' is reported, the Storage Device wraps the secret (or a key that wraps the secret) with the authentication values of authorized users (and possibly also other protections as well).

Q. Which value is 'better'?
A. The specification is intentionally flexible to allow for device vendors to implement alternative architectures that balance factors such as assurance, complexity, and functionality.

Q. What is the relationship between this value and the locking state of the device?
A. Even where a device applies strong mechanisms to protect secrets, those protections may be intentionally bypassed if the device is configured so that it is unlocked for either reading or writing of a specific LBA range prior to authentication (because the device needs to be able to read or write to the range). For strong protection of data at rest against unauthorized disclosure, an independent software vendor supporting the Storage Device would simply not configure ranges to be unlocked for reading or writing prior to authentication.

Q. If the Storage Device does not report this value, how can I tell how the media encryption key is protected?
A. For Storage Devices that do not report this value, please contact the device vendor (not the TCG) for information about how critical security parameters are protected by the device.

Contact: Anne Price
602-840-6495
press@trustedcomputinggroup.org