TCG Storage
Protection Mechanisms for Secrets

Specification Version 1.00
Revision 1.00
05 March, 2012

Contacts:

storagewg@trustedcomputinggroup.org

TCG Published

TCG

Change History

Version 1.00	Date	Description
Revision 1.00	March 5, 2012	First Publication

TABLE OF CONTENTS

Tables

1 Introduction

1.1 Document Purpose

The Storage Workgroup specifications provide a comprehensive architecture for putting Storage Devices under policy control as determined by the trusted platform host, the capabilities of the Storage Device to conform with the policies of the trusted platform, and the lifecycle state of the Storage Device as a Trusted Peripheral.

[2] defines the `SecretProtect` table used for reporting the mechanisms supported by a trusted Storage Device for protecting key material and secrets. The `SecretProtect` table's `ProtectMechanisms` column contains a set of protection mechanisms that the Storage Device supports. This document defines the values that MAY be reported in the `ProtectMechanisms` column, and their meanings.

1.2 Scope and Intended Audience

This specification defines the mechanisms for protecting key material and secrets that a trusted Storage Device may report that it supports.

The intended audience for this specification is both trusted Storage Device manufacturers and developers that want to use these Storage Devices in their systems.

1.3 Key Words

Key words are used to signify SSC requirements.

The Key Words "**SHALL**", "**SHALL NOT**", "**SHOULD**," and "**MAY**" are used in this document. These words are a subset of the RFC 2119 key words used by TCG, and have been chosen since they map to key words used in T10/T13 specifications. These key words are to be interpreted as described in [1].

1.4 Document References

[1]. IETF RFC 2119, 1997, "Key words for use in RFCs to Indicate Requirement Levels"

[2]. Trusted Computing Group (TCG), "TCG Storage Architecture Core Specification", Version 2.00

2 Protection Mechanisms for Secrets

Table 1 defines the values that are reported by a trusted Storage Device in the `ProtectMechanisms` column of the `SecretProtect` table as defined in [2], the meaning of each value, and if the protection mechanism is a cryptographic protection, physical protection, or a combination of cryptographic and physical protection. The values reported correspond to the protection mechanism(s) employed when the access control configuration for the key is in its strictest configuration.

Table 1 `ProtectMechanisms` Column Set Values

Set Value	Associated Value	Meaning	Cryptographic or Physical Protection
0	Vendor Unique	Key material/secrets are protected with a vendor-unique protection scheme	Vendor Unique
1	Authentication Data Required	The key(s), or intermediate key(s) that encrypt those key(s), are encrypted with the authorized user's `C_PIN` object's `PIN` value (or a key derived from the `PIN` value) such that the key(s) are protected with the level of entropy provided by the `PIN` value.	Cryptographic