

TCG Storage Protection Mechanisms for Secrets

Specification Version 1.00
Revision 1.00
05 March, 2012

Contacts:

storagewg@trustedcomputinggroup.org

TCG Published

TCG

Copyright © TCG 2012

Copyright © 2011 Trusted Computing Group, Incorporated.

Disclaimer

THIS SPECIFICATION IS PROVIDED "AS IS" WITH NO WARRANTIES WHATSOEVER, INCLUDING ANY WARRANTY OF MERCHANTABILITY, NONINFRINGEMENT, FITNESS FOR ANY PARTICULAR PURPOSE, OR ANY WARRANTY OTHERWISE ARISING OUT OF ANY PROPOSAL, SPECIFICATION OR SAMPLE. Without limitation, TCG disclaims all liability, including liability for infringement of any proprietary rights, relating to use of information in this specification and to the implementation of this specification, and TCG disclaims all liability for cost of procurement of substitute goods or services, lost profits, loss of use, loss of data or any incidental, consequential, direct, indirect, or special damages, whether under contract, tort, warranty or otherwise, arising in any way out of use or reliance upon this specification or any information herein.

No license, express or implied, by estoppel or otherwise, to any TCG or TCG member intellectual property rights is granted herein.

Except that a license is hereby granted by TCG to copy and reproduce this specification for internal use only.

Contact the Trusted Computing Group at www.trustedcomputinggroup.org for information on specification licensing through membership agreements.

Any marks and brands contained herein are the property of their respective owners.

Change History

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

TABLE OF CONTENTS

| | | |
|----------|--|----------|
| 1 | INTRODUCTION | 6 |
| 1.1 | DOCUMENT PURPOSE | 6 |
| 1.2 | SCOPE AND INTENDED AUDIENCE | 6 |
| 1.3 | KEY WORDS | 6 |
| 1.4 | DOCUMENT REFERENCES | 6 |
| 2 | PROTECTION MECHANISMS FOR SECRETS | 7 |

Tables

Table 1 ProtectMechanisms Column Set Values 7

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 <code>C_PIN</code> object's <code>PIN</code> value (or a key derived from the <code>PIN</code> value) such that the key(s) are protected with the level of entropy provided by the <code>PIN</code> value. | Cryptographic |