TCG Storage Feature Set: Block SID Authentication

Specification Version 1.00 Published
Revision 1.00

August 5, 2015

Contact: admin@trustedcomputinggroup.org

TCG

PUBLISHED

Disclaimers, Notices, and License Terms

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.

1.2 Scope and Intended Audience

This specification defines the Block SID Authentication Feature. Any Storage Device that claims Block SID Authentication compatibility SHALL conform to this specification.

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].

In addition to the above key words, the following are also used in this document to describe the requirements of particular features, including tables, methods, and usages thereof.

- **Mandatory (M):** When a feature is Mandatory, the feature SHALL be implemented. A Compliance test SHALL validate that the feature is operational.
- **Optional (O):** When a feature is Optional, the feature MAY be implemented. If implemented, a Compliance test SHALL validate that the feature is operational.
- **Excluded (X):** When a feature is Excluded, the feature SHALL NOT be implemented. A Compliance test SHALL validate that the feature is not operational.
- **Not Required (N)** When a feature is Not Required, the feature MAY be implemented. No Compliance test is required.

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 2.01

[3]. Trusted Computing Group (TCG), "TCG Storage Security Subsystem Class: Opal", Version 1.00

[4]. Trusted Computing Group (TCG), "TCG Storage Security Subsystem Class: Opal", Version 2.00

[5]. Trusted Computing Group (TCG), "TCG Storage Security Subsystem Class: Opal", Version 2.01

[6]. Trusted Computing Group (TCG), "TCG Storage Security Subsystem Class: Opalite", Version 1.00

[7]. Trusted Computing Group (TCG), "TCG Storage Security Subsystem Class: Pyrite", Version 1.00

[8]. Trusted Computing Group (TCG), "TCG Storage Storage Interface Interactions Specification", Version 1.04

1.5 Document Precedence

In the event of conflicting information in this specification and other documents, the precedence for requirements is:

1. This specification and [3] or [4] or [5] or [6] or [7] (this document and an SSC are at the same level of precedence, and SHALL NOT conflict with each other)
2. Storage Interface Interactions Specification [8]
3. TCG Storage Architecture Core Specification [2]

1.6 Dependencies on Other Feature Sets

This feature set has no dependencies on other feature sets.

1.7 Interactions with Other Feature Sets

This feature set has no interactions with other feature sets.

2 Block SID Authentication Overview

Begin Informative Content

This specification defines a mechanism by which a host application can alert the storage device to block attempts to authenticate the SID authority until a subsequent device power cycle occurs.

This mechanism can be used by BIOS/platform firmware to prevent a malicious entity from taking ownership of a SID credential that is still set to its default value of MSID.

End Informative Content

3 SSC Specific Functionality

This feature set requires no additional SSC-specific functionality.

4 Feature Set Requirements

This section defines the Mandatory (M) and Optional (O) requirements for the Block SID Authentication Feature Set.

4.1 Level 0 Discovery

A SD that implements the Block SID Authentication Feature Set SHALL return the Block SID Authentication Feature Descriptor as described in 4.1.1, in addition to the Level 0 Discovery response requirements defined in other applicable specifications.

4.1.1 Block SID Authentication (Feature Code = 0402)

This feature descriptor SHALL be returned when the SD supports the Block SID Authentication Feature Set. The contents of the feature descriptor are defined in Table 1.

Table 1 Level 0 Discovery – Block SID Authentication

Byte \ Bit	7	6	5	4	3	2	1	0
0	(MSB)							
1	Feature Code							(LSB)
2	Version				Reserved			
3	Length							
4	Reserved						SID Blocked State	SID Value State
5	Reserved							Hardware Reset
6-15	Reserved							

4.1.1.1 SID Value State

This field specifies whether the C_PIN_SID object's PIN column value is equal to the C_PIN_MSID object's PIN column value.

1. This bit SHALL be 0 if the C_PIN_SID object's PIN column value is equal to the C_PIN_MSID object's PIN column value.
2. This bit SHALL be 1 if the C_PIN_SID object's PIN column value is not equal to the C_PIN_MSID object's PIN column value.

4.1.1.2 SID Blocked State

This field specifies whether the authentication of the SID feature is blocked (see 4.2.2).

1. This bit SHALL be 0 if authentication of the SID authority is not blocked due to the Block SID Authentication command.
2. This bit SHALL be 1 if authentication of the SID authority is currently blocked due to the Block SID Authentication command.

4.1.1.3 Hardware Reset

This bit SHALL be 1 if a Hardware Reset was selected to be able to clear the SID Authentication block.

Begin Informative Note

The following events are always Clear Events, and as such there is no field in Level 0 discovery identifying that either has been selected as a Clear Event:

1. Power Cycle
2. Revert

End Informative Note

4.1.1.4 Level 0 requirements for the Block SID Authentication Feature Set

1. **Feature Code**: 0x0402
2. **Version**: 0x1 or any version that supports the defined features in this specification
3. **Length**: 0x0C

4.2 Block SID Authentication Command (M)

4.2.1 Command Structure and Execution

The Block SID Authentication command is delivered by the transport IF-SEND command.

If the Block SID Authentication command is supported, the TPer SHALL accept and acknowledge it at the interface level.

If the Block SID Authentication command is not supported, the TPer SHALL abort attempted invocations of the command at the interface level with the “Other Invalid Command Parameter” status (see [8]).

There is no IF-RECV response to the Block SID Authentication command.

The Block SID Authentication command is defined in Table 2.

1. The Transfer Length SHALL be non-zero. Transferred data is formatted as indicated in Table 2.
2. The Clear Events field identifies the SD resets that clear the SID Authentication block and allow the SID authority to be able to be authenticated as normal. See Table 3 for the structure of the Clear Events field.

Table 2 Block SID Authentication Command

FIELD	VALUE
Command	IF-SEND
Protocol ID	0x02
Transfer Length	Non-zero
ComID	0x0005
Byte 0	Clear Events (see Table 3)
Bytes 1 to Transfer Length – 1	Reserved (00)

4.2.2 Command Operation

If the SID C_PIN credential is not the same as the value of the MSID C_PIN credential, then:

1. The Block SID Authentication command SHALL result in success but SHALL have no effect.

If the SID C_PIN credential is the same as the value of the MSID C_PIN credential, then:

1. Upon successful execution of the Block SID Authentication Command and until the next applicable SD Clear Event:
    a. Otherwise valid invocations of the Authenticate method in which the Authority parameter is the SID authority's UID SHALL result in a method status of SUCCESS, and a method result of False.
    b. Otherwise valid invocations of the StartSession method in which the HostSigningAuthority parameter is the SID authority's UID SHALL result in a SyncSession method with a status of NOT AUTHORIZED.
    c. The Tries column of the SID C_PIN credential SHALL NOT be incremented as a result of authentication attempts that were unsuccessful due to the Block SID Authentication.

If a Block SID Authentication command has been successfully executed and SID authentication is blocked:

1. Subsequent invocations of the Block SID Authentication command SHALL fail with status "Other Invalid Command Parameter", and
2. The SID Blocked State SHALL NOT change, and
3. Clear Events in effect SHALL remain the same as identified in the most recent successful invocation of the Block SID Authentication command.

After an applicable Clear Event occurs, attempts to authenticate the SID authority SHALL be processed normally until the Block SID Authentication command is successfully executed.

Clear Events selected by the successful execution of the Block SID Authentication command are reset when a Clear Event occurs.

4.2.3 Clear Events

Clear Events are mechanisms that reset the state of the SID Authentication Block, in order to permit normal authentication of the SID authority. Clear Events also reset the current selection of host-selectable Clear Events.

The following SHALL always be Clear Events, and upon their occurrence SHALL clear the SID Authentication Block and reset the selection of Clear Events:

1. A SD Power Cycle. See [8] for a mapping of TCG Storage Power Cycle reset type to resets defined by the underlying interface.
2. A successful invocation of the Revert method on the Admin SP's object in the Admin SP's SP table. See [3], [4], [5], [6], and [7] for SSC-specific definitions of the Revert method.

The following possible Clear Events MAY be selected by the host during execution of the Block SID Authentication:

1. Hardware Reset. See [8] for a mapping of TCG Storage Hardware Reset reset type to resets defined by the underlying interface.
    a. A host selects Hardware Reset as a Clear Event by setting the Hardware Reset bit (Table 3) to 1 when invoking the Block SID Authentication command.

After a successful invocation of the Block SID Authentication command:

1. Any default Clear Events (e.g. Power Cycle, Revert) SHALL clear the SID Authentication Block.
2. Any Clear Events supported by the device and selected in the command SHALL clear the SID Authentication Block.
3. The Clear Events selected by that command SHALL NOT be modifiable by subsequent invocations of the Block SID Authentication command until after a Clear Event has occurred (see 4.2.2).

Table 3 Clear Events

Byte \ Bit	7	6	5	4	3	2	1	0
0	(MSB) Reserved							Hardware Reset (LSB)

4.3 Admin SP

This feature set requires no additions to the Admin SP.

4.4 Locking SP

This feature set requires no additions to the Locking SP.

4.5 Additional SPs

This feature set requires no additional SPs.