SD Specifications
Part 1
Extended Security Simplified Addendum
(Using SECURE_RECEIVE/SEND Commands)

Version 1.00

November 30, 2022

Addendum to:

SD Specifications
Part 1 Physical Layer Specification
Version 9.00 February 10, 2022 or later

Technical Committee
SD Card Association

Revision History

Date	Version	Changes compared to previous issue
Nov 30, 2022	1.00	The first release of Extended Security Simplified Addendum

Conditions for publication

Publisher:

SD Card Association
2400 Camino Ramon, Suite 375
San Ramon, CA 94583 USA
Telephone: +1 (925) 275-6615,
Fax: +1 (925) 886-4870
E-mail: help@sdcard.org

Copyright Holder:

The SD Card Association

Notes:

The copyright of the previous versions (Version 1.00 and 1.01) and all corrections or non-material changes thereto are owned by SD Group.
The copyright of material changes to the previous versions (Version 1.01) are owned by SD Card Association.

Disclaimers:

This Simplified Specification is made available by the SD Card Association (the "SDA") at https://www.sdcard.org/downloads/pls/index.html (the "Site") and your access to and/or use of this Simplified Specification is subject to the SIMPLIFIED SPECIFICATION TERMS AND CONDITIONS (the "Terms") that are displayed by clicking the "Download" button at https://www.sdcard.org/downloads/pls/index.html.

If you are viewing or have accessed this Simplified Specification via any source, medium, or in any other way other than directly from the Site pursuant your acceptance of the Terms, then your access to, viewing of, and/or use of the Simplified Specification is in violation of the SDA's and its licensors' intellectual property rights. Accordingly, unless obtained directly from the Site pursuant to the Terms, immediately cease and desist all viewing, using, or accessing the Simplified Specification; destroy any copies of the Simplified Specification in your possession, custody or control; and, if you desire access to the Simplified Specification, proceed to the Site to obtain access and use of the Simplified Specification in an authorized manner pursuant to the Terms.

Distribution of the Simplified Specification, other than through the Site, is a violation of the Terms and the intellectual property rights of the SDA and its licensors. The only rights granted in the Simplified Specification are those expressly granted in the Terms. All rights not expressly granted pursuant to your acceptance of the Terms are reserved to the SDA and its licensors. Notice is also hereby provided that notwithstanding any rights granted by the Terms, any implementation of the Simplified Specifications or any portions thereof may require a separate license from the SDA, SD Group, SD-3C, LLC or other third parties.

Conventions Used in This Document

Naming Conventions

- Some terms are capitalized to distinguish their definition from their common English meaning.
- Words not capitalized retain their common English meaning.

Numbers and Number Bases

- Hexadecimal numbers are written with a lower case "h" suffix, e.g., FFFFh and 80h.
- Binary numbers are written with a lower case "b" suffix (e.g., 10b).
- Binary numbers larger than four digits are written with a space dividing each group of four digits, as in 1000 0101 0010b.
- All other numbers are decimal.

Key Words

- May: Indicates flexibility of choice with no implied recommendation or requirement.
- Shall: Indicates a mandatory requirement. Designers shall implement such mandatory requirements to ensure interchangeability and to claim conformance with the specification.
- Should: Indicates a strong recommendation but not a mandatory requirement. Designers should give strong consideration to such recommendations, but there is still a choice in implementation.

Application Notes

Some sections of this document provide guidance to the host implementers as follows:

Application Note: This is an example of an application note.

Table of Contents

Table of Tables

1. General

The Extended Security Addendum specification was prepared as addendum to SD Specifications Part 1 Physical Layer Specification Ver 9.0 (SD 9.0).

Two commands were introduced in SD 9.0: SECURE_RECEIVE (ACMD53) and SECURE_SEND (ACMD54) enabling new infrastructure of pass-through commands allowing the transfer of other protocols over the SD standard protocol.

This Extended Security Addendum specification describes the requirements to implement security functionality of TCG in an SD card.

2. SD Security Data Transport Requirements

2.1 Extended Security Commands

ACMD53 (SECURE_RECEIVE) command and ACMD54 (SECURE_SEND) command has been defined in SD 9.0 for security data transport between the host and SD Card that supports the T10/BSR INCITS security protocol.

Support of the SECURE_RECEIVE and SECURE_SEND Commands is mandatory to support the Extended Security Addendum as specified in this document. Refer to SD 9.0 or later releases.

Support bit for ACMD53/54 commands is assigned to SCR bit 36.

Support bit for TCG is assigned to SCR bit 45.

2.2 Discovery of Extended Security Commands Support

The host issues ACMD51 SEND_SCR command to obtain the SD Configuration Register (SCR).

- Bit 36 of SCR field shall return a value of '1' to indicate support of SECURE_RECEIVE and SECURE_SEND commands.
- Bit 45 of SCR register shall return value of '1' to indicate that TCG is supported by the card.

2.3 Atomicity of Extended Security Commands

ACMD53 and ACMD54 commands are required to be preceded by CMD23 SET_BLOCK_COUNT command. Each CMD23/ACMD53 or CMD23/ACMD54 commands combination shall be considered as atomic, similar to pre-defined block count Read and Write commands.

A CMD23/ACMD53 or CMD23/ACMD54 commands combination are necessary to transmit the information corresponding to the Security Protocol.

Issuing ACMD53 command or ACMD54 command without a preceding CMD23 command shall result in a SECURE_CMD_STATUS error as defined in SD 9.0.

2.4 Data transport requirements specific to this Security Extension Specification

The data transport payload sizes are limited by SD specification to increments of 512 bytes (e.g., a block count value of one means 512 bytes, two means 1024 bytes, etc.). If additional bytes are required to meet these size requirements, then pad bytes shall be appended to meet this length. Pad bytes shall have a value of 00h.

In SD 9.0 and later, CMD23 is supported with ACMD53/54 for all SD Card capacity types including SDSC cards. Usage of CMD23 set the Block Count assuming block length of 512 Bytes, also for SDSC cards, ignoring block length set by CMD16.

2.5 SECURE_RECEIVE and SECURE_SEND Commands usage for TCG

ACMD53 command (SECURE_RECEIVE) and ACMD54 command (SECURE_SEND) are used to transfer various protocols over SD.

TCG protocol is transferred over SD Card protocol in a transparent manner using the two commands ACMD53 and ACMD54.

Bit Byte	7	6	5	4	3	2	1	0
0	[47] Start Bit	[46] Transition Bit	[45:40] Command Index					
1	[39:32] Security Protocol (*as defined in* INCITS 513-2015 SPC-4 *for TCG Security Protocol code*)							
2	[31:24] Security Protocol Specific (15:08) (*as defined in TCG spec*)							
3	[23:16] Security Protocol Specific (07:00) (*as defined in TCG spec*)							
4	[15:08] Reserved							
5	[07:01] CRC7							[0] Stop Bit

Table 2-1 SECURE_RECEIVE and SECURE_SEND commands Structure

The type of protocol transferred over these two commands is defined in the Security Protocol field (refer to Byte #1 shown at Table 2-1).
The Security Protocol field is as defined in INCITS 513-2015 SPC-4 (T10).

This is done in similar manner to the usage of TCG over NVMe and/or SATA allowing similar implementation of TCG either through the SD interface or through the PCIe interface in case of SD Express cards.
Description here is a blank in the Simplified Specification.

3. TCG Storage Security Functional Requirements

3.1 TCG Storage Security overview

The TCG Storage Security specifications define an architecture that puts storage devices under the policy control of a trusted platform host.

- The TCG Storage Core specification [TCGCore] provides a general security framework.
- The TCG Storage Security Subsystem Class (SSC) Ruby v1.0 [TCGRuby] provides a specific functional security set.
- The TCG Storage Additional DataStore Tables Feature Set [TCGAddDST] adds specific functionality to the Ruby SSC.
- The TCG Storage Single User Mode Feature Set [TCGSUM] adds optional specific functionality to the Ruby SSC.
- The TCG Storage Interface Interaction specification [TCGSIIS] provides a description of the functional interactions between the security subsystem and the external interface (e.g., SD Card) functionality.

3.2 Requirements for the TCG Storage Core in the SD Card security extension

An SD device, compliant with this standard, shall implement TPer functionalities defined in [TCGCore] required to support: [TCGRuby] and [TCGAddDST]. In particular, it shall support:

- The Locking Feature (0x0002);
- The TCG Stack reset; and
- The following Session Manager methods:
    - TPer Properties Method;
    - Start Session Method;
    - Close Session Method;
    - Sync Session Method.

The device is not required to support the following features:

- Asynchronous protocol communication
- Creation or deletion of tables, and creation or deletion of table rows post-manufacturing

3.3 Requirements for the TCG Storage Ruby SSC in the SD Card security extension

An SD Card which supports TCG shall support the TCG Storage Ruby SSC specification (see [TCGRuby]) and in particular:

- Geometry Reporting Feature in level 0 Discovery;
- ability to disable SID authority in the Admin SP; and
- the Locking SP shall be created by the device manufacturer.

The device is not required to support the following features:

- Dynamic ComID Management;
- RestrictedCommands (Object Table)

3.3.1 Level 0 Discovery

SD Cards, compliant with this standard, shall return the following elements in the Level 0 response as defined in [TCGRuby]:

- Level 0 Discovery Header
- TPer Feature Descriptor
- Locking Feature Descriptor
- Ruby SSC Feature Descriptor

• Geometry Reporting

3.3.1.1 Level 0 Discovery Header

See [TCGRuby].

3.3.1.2 TPer Feature (Feature Code = 0x0001)

SD Cards, compliant with this standard, are not required to support: ComID management, buffer management, ACK/NACK, Asynchronous protocol.
Table 3-1 is informative and shows Level 0 Discovery - TPer Feature Descriptor content for a device implementing the required features only.

Byte \ Bit	7	6	5	4	3	2	1	0
0	(MSB)	Feature Code (0x0001)						
1								(LSB)
2	Version				Reserved			
3	Length = 0x0C							
4	Reserved	ComID Mgmt Supported = 0	Reserved	Streaming Supported = 1	Buffer Mgmt Supported = 0	ACK/NAK Supported = 0	Async Supported = 0	Sync Supported = 1
5 - 15	Reserved							

NOTE 1 Version = 0x1 or any version that supports the defined features in [TCGRuby].

Table 3-1 Level 0 Discovery - TPer Feature Descriptor

3.3.1.3 Locking Feature (Feature Code = 0x0002)

See [TCGRuby].

3.3.1.4 Geometry Reporting Feature (Feature Code = 0x0003)

This section defines requirements for some parameters of Geometry Reporting Feature Descriptor.

Align
For SD Cards, compliant with this standard, the value of the AlignmentRequired column of the LockingInfo table shall be equal to TRUE, therefore the ALIGN bit shall be set to one.

LogicalBlockSize
LogicalBlockSize indicates the number of bytes in a logical block.
LogicalBlockSize shall be set according to Table 3-2.

READ_BL_PARTIAL field and WRITE_BL_PARTIAL field of the device CSD register shall be set to zero.

Device Capacity Range	SD Specification		Geometry Reporting Feature Fields	
	Native Sector size	Address Mode	LogicalBlockSize	Alignment Granularity
Capacity ≤ 2 GByte	N.A	Byte (1)	1	512 * 2^N, with N≥0
Capacity > 2 GByte	512 Byte	512 Byte	512	2^N, with N≥0
Capacity > 2 GByte	4 Kbyte(3)	512 Byte (2)	512	8 * 2^N, with N≥0

NOTE 1 For Capacity not greater than 2 GByte, the address shall be aligned to 512-Byte even though the device is byte addressable.
NOTE 2 For Capacity greater than 2 GByte, the address shall be aligned to 8 512-Byte sector, and the data transfer shall be a multiple of 8 512-Byte sector.
NOTE 3 Applicable only in NVMe mode.

Table 3-2 LogicalBlockSize and AlignmentGranularity

AlignmentGranularity
See [TCGRuby]. Please note that the term “physical block” referenced in [TCGRuby] is not to be confused with the “erase group” definition in SD Specification. Instead, it refers to a physical property of the storage medium specific to the manufacturer for the purpose of logical to physical mapping optimization.
This parameter is vendor unique and its value shall set as defined in Table 3-2.

LowestAlignedLBA
Lowest-Aligned-LBA indicates the lowest logical block address that is located at the beginning of an alignment granularity group. For SD Cards compliant with this standard LowestAlignedLBA shall be set to zero.

Geometry Reporting Feature Descriptor
Table 3-3 is informative and shows Level 0 Discovery - Geometry Descriptor content for a device implementing the required features only.

Byte \ Bit	7	6	5	4	3	2	1	0
0	(MSB)	Feature Code (0x0003)						
1								(LSB)
2	Version				Reserved			
3	Length = 0x1C							
4	Reserved							ALIGN = 1
5		Reserved						
6								
7								
8								
9								
10								
11								
12	(MSB)	LogicalBlockSize						
13								
14								
15								(LSB)
16	(MSB)	AlignmentGranularity						
17								
18								
19								
20								
21								
22								
23								(LSB)
24	(MSB)	LowestAlignedLBA						
25								
26								
27								
28								
29								
30								
31								(LSB)

NOTE 1 Version = 0x1 or any version that supports the defined features in [TCGRuby].

Table 3-3 Level 0 Discovery - Geometry Reporting Feature Descriptor

3.3.1.5 Ruby SSC V1.00 Feature (Feature Code = 0x0304)

Devices compliant with this standard shall support:

- at least the following two ComID values:
  - 0x0001 (Level 0 Device Discovery)
  - 0x0004 (TPER_RESET command)
- Range Crossing
  - The device supports commands addressing consecutive LBAs in more than one LBA range if all the LBA ranges addressed are unlocked.
- at least one (1) Locking SP Admin Authorities
- at least two (2) Locking SP User Authorities

NOTE Support for more than two (2) Locking SP User Authorities is implementation specific; therefore it may not be provided by all devices in the market.

In addition to the previous requirements, the “Initial C_PIN_SID PIN Indicator” field and “Behavior of C_PIN_SID PIN upon TPer Revert” field shall be set to zero (see [TCGRuby)].

A part of this section is not described in the simplified version.

3.3.2 Properties Requirements

The requirements for support of the various properties, and the requirements for their values, are shown in Table 3-5.

Property Name	Property Requirements and Values Reported
MaxComPacketSize	16384 (minimum)
MaxResponseComPacketSize	16384 (minimum)
MaxPacketSize	16384 (minimum)
MaxIndTokenSize	16328 (minimum)
MaxPackets	1
MaxSubPackets	1
MaxMethods	1
MaxSessions	1
MaxAuthentications	2
MaxTransactionLimit	1
DefSessionTimeout	

Table 3-5 Property Requirements

3.4 Requirements for the TCG Storage DataStore Tables feature set in SD Card

An SD card which supports TCG shall support the “TCG Storage Opal SSC Feature Set: Additional DataStore Tables” specification [TCGAddDST] with the following requirements:

• The number of the DataStore Tables shall be equal to or greater than the number of Locking SP User Authorities reported in the Ruby SSC V1.00 Feature Descriptor;
• The total size of the DataStore Tables shall be at least 10MByte.

3.4.1 DataStore Table Feature Descriptor (Feature Code = 0202h)

This descriptor shall be returned by devices compliant with this standard.
The maximum number of the DataStore Tables shall be equal to or greater than the number of Locking SP User Authorities reported in the Ruby SSC V1.00 Feature Descriptor (see 3.3.1.5).
As required by [TCGRuby], the maximum total size of DataStore tables shall be at least 10MByte.
Table 3-6 is informative and shows Level 0 Discovery - DataStore Table Feature Descriptor content for a device implementing the minimum requirements described in this standard.

Byte \ Bit	7	6	5	4	3	2	1	0
0	(MSB)			Feature Code = 0x0202h				
1								(LSB)
2	Version				Reserved			
3	Length = 0x0C							
4	Reserved							
5	Reserved							
6	(MSB)			Maximum number of DataStore tables = 0x0008				
7								(LSB)
8	(MSB)			Maximum total size of DataStore tables = 0x0000 0000 00A0 0000				
9								
10								
11								(LSB)
12	(MSB)			Minimum DataStore table size alignment = 1 or above				
13								
14								
15								(LSB)

NOTE 1 Version = 0x1 or any version that supports the defined features in [TCGRuby].

Table 3-6 Level 0 Discovery - DataStore Table Feature Descriptor

3.5 Requirements for the TCG Storage Support Single User Mode feature set in the SD Card

An SD card which supports TCG may support the “TCG Storage Opal SSC Feature Set: Single User Mode Specification” [TCGSUM].

3.6 Requirements for security characteristics for SD Card

This section is a blank in the Simplified Specification.

3.7 Requirements for MBR Shadowing Support

An SD card which supports TCG shall support MBR shadowing as defined in [TCGCore] spec and in [TCGSIIS] spec. Control of MBR Shadowing is compliant to “MBRControl Table” defined in [TCGCore]. More detailed information on the MBR shadowing specification in SD cards is provided in SD 9.0 .

4. Security Interactions with SD Card Operations

4.1 Security Support Restrictions on Partitions

The extended security functionality described in this document shall have effects on the User Partition only. All other partitions shall operate as in an SD Card without extended security functions.

ACMD53 SECURE_RECEIVE and ACMD54 SECURE_SEND commands are accepted while the device is operating in User Partition mode only. ACMD53 and ACMD54 issued while the device is operating in a different partition shall be considered as illegal commands.

ACMD53 and ACMD54 are used to transfer the TPer commands in accessing the MBR while MBR shadowing is active as defined in [TCGCore] (Section 5.7.2.5.2).

Also note that RPMB is considered as ‘unit’. Not a partition. ACMD53 and ACMD54 are used to access the RPMB as well.

4.2 Authentication and Access Control Management on User Partition

If the TCG security feature is implemented, user authentication and access control to the User Partition is managed per TCG security (see SD 9.0).

4.3 TCG Interaction with SD Card Write Protect States

TCG and Write Protect functions may be operated at the same time. If both TCG security feature and card Write Protection are implemented and enabled, then access to user area is restricted as defined in SD 9.0 and in [TCGSIIS] spec.

4.4 TCG Interaction with SD Card PWD Lock Function

TCG and PWD Lock functions may be operated at the same time. If both TCG security feature and PWD Lock Protection are implemented and enabled, then access to user area is restricted as defined in SD 9.0 and in [TCGSIIS] spec.

Forced Erase operation will erase the PWD (of PWD Lock function) and all the user data except the TCG MBR Table.

TCG Revert operation will bring the SD Card to its original factory state (i.e., erase the TCG password and all the user data as defined in [TCGCore] spec).

COP (Card Ownership Protection) and TCG functions are mutually exclusive – that means that if the SD Card supports the COP function and it is enabled, then TCG security feature cannot be enabled and if TCG security feature is enabled, then COP cannot be enabled (Refer to SD 9.0 for more information).

5. Error Handling

5.1 Secure Command Status in SD Status

TPer error ID will be identified using the 3 bits of SECURE_CMD_STATUS in SD Status register (bits [498:496]) as shown in Table 5-1.

Value	Status code	Description
00h	Successful Completion	The command completed without error.
01h	Invalid Field in Command	A reserved coded value or an unsupported value in a defined field (other than the opcode field). This status code should be used unless another status code is explicitly specified for a particular condition. The field may be in the command parameters as part of the submission queue entry or in data structures pointed to by the command parameters.
02h	Command Sequence Error	The command was aborted due to a protocol violation in a multi-command sequence (e.g., a violation of the Security Send and Security Receive sequencing rules in the TCG Storage Synchronous Interface Communications protocol (refer to TCG Storage Architecture Core Specification)).
03h	Access Denied	Access to the namespace and/or user data is denied due to lack of access rights. Refer to the appropriate security specification (e.g., TCG Storage Interface Interactions Specification).
04h-07h	Reserved	

Table 5-1 Error codes as represented by SECURE_CMD_STATUS in SD Status register

The Invalid Security Protocol ID Parameter error will be represented with value “01h” (‘Invalid Field in Command’) in SECURE_CMD_STATUS. Such indication means that direct communications with the TPer are not being processed correctly due to invalid Protocol ID field value in SECURE_SEND command or SECURE_RECEIVE command. Other error indications are represented using this SD Status field. The relation between the various TPer errors and the SECURE_CMD_STATUS indication is defined in [TCGSIIS].

5.2 Unauthorized Access

Unauthorized access is an application error defined and reported by the SD Card. The application relationship is described in [TCG SIIS]. No data shall be written to or read from the medium.
Restrictions and device behaviors for access across secure LBA ranges are described in [TCGRuby].
Unauthorized access is reported as a Data Protection Error.
For SD Card, the Data Protection Error as defined in [TCG SIIS] is reported in the SECURE_CMD_STATUS indicating ‘Access Denied’ (value ‘03h’ in the SECURE_CMD_STATUS) in the SD Status register.

6. Configuration

6.1 SD Card Partition Configuration

An SD Card that supports TCG shall designate the User partition as the TCG Ruby-SSC compliant storage device (SD), supporting one TCG secure storage TPer.

Note that Shadow MBR is also part of the user partition and is operable/accessed according to the boot status condition, as defined in SD 9.0.

The storage TPer shall contain the Manufactured SP's (Admin SP and Locking SP) in the Manufactured-Inactive state as shipped from the device manufacturer. The User partition cannot be re-configured once the Manufactured SP's have transitioned from Manufactured-Inactive to Manufactured state.

Appendix A (Normative): Reference

This specification refers the following documents:
1) Part 1 Physical Layer Specification Version 9.00 or later

Also -
The following normative documents contain provisions that, through reference in this text, constitute provisions of this standard. For dated references, subsequent amendments to, or revisions of, any of these publications do not apply. However, parties to agreements based on this standard are encouraged to investigate the possibility of applying the most recent editions of the normative documents indicated. For undated references, the latest edition of the normative document referred to applies.
2) Trusted Computing Group [TCGCore], TCG Storage Architecture Core Specification, Version 2.01, Revision 1.00
3) Trusted Computing Group [TCGRuby], TCG Storage Security Subsystem Class: Ruby Specification, Version 1.00, Revision 1.00
4) Trusted Computing Group [TCGAddDST], TCG Storage Opal SSC Feature Set: Additional DataStore Tables Specification, Version 1.00, Revision 1.00
5) Trusted Computing Group [TCGSUM], TCG Storage Opal SSC Feature Set: Single User Mode Specification, Version 1.00, Revision 2.00
6) Trusted Computing Group [TCGSIIS], TCG Storage Interface Interactions Specification (SIIS), Version 1.11 (r1.0).
7) INCITS 513-2015 SPC-4 (T10)

A.1 TCG Security Methods vs TCG in SD Card

The following table describes the features in Ruby SSC 1.0 and the adjusted features for SD 9.0. The main changes are with making the MBR as mandatory, requiring DataStore of 10MB and mandating the Additional Datastore tables Feature Set.

Support for Feature	Opal 2.01	Ruby 1.00 SSC	Ruby 1.00 SSC For SD Card
MBR	Mandatory (128MB)	Optional	Mandatory
Datastore	10MB	128K	10MB
Additional Datastore tables Feature Set	Mandatory	Not Specified	Mandatory
Number of Locking SP Admins/Users	4 Admin, 8 User	1 Admin, 2 User	1 Admin, 2 User
Req'd locking ranges	Global + 8	Global only	Global only
AdminSP Authorities	SID, Makers, 1 Admin and PSID	SID, Makers, 1 Admin / 1PSID	SID, Makers, 1 Admin / 1PSID
Revert, RevertSP, Erase	Revert, RevertSP	Revert, Revert SP (= Erase)	Revert, Revert SP (= Erase)
Core spec & encoding	V2.01	V2.01	V2.01
# of ComPackets, Packets, SubPackets per transfer	1/1/1 min; more optional	1/1/1 min; more optional	1/1/1 min; more optional
# of ComID	1	1	1
Life cycle management	Mandatory	Mandatory	Mandatory
Configurable Access Control	Mandatory	Mandatory	Mandatory
Block SID FS	Not Specified	Mandatory	Mandatory
Single User Mode Feature Set	Not Specified	Optional	No Support
Configurable Namespace Locking FS	Not Specified	Optional	No Support
PSK Secure Msg Feature Set	Not Specified	Optional	No Support
Geometry info in Locking SP and Level 0 discovery	Optional	Optional	No Support

Table A-1 TCG Common Security Methods and the Method Defined for SD