SD Association

Boot, TCG and RPMB – The New Security Features Introduced in SD 9.0

White Paper | March 2022

www.sdcard.org | ©2022 SD Association. All rights reserved

Conditions for publication

Publisher and Copyright Holder:

SD Card Association
5000 Executive Parkway, Suite 302
San Ramon, CA 94583 USA
Telephone: +1 (925) 275-6615
Fax: +1 (925) 886-4870
E-mail: help@sdcard.org

Disclaimers:

The information contained in this whitepaper is provided as is without any representations or warranties of any kind. No responsibility is assumed by the SD Association for any damages, or any infringements of patents or other rights of the SD Association or any third parties, which may result from the use of any portion thereof. No license is granted by implication, estoppel or otherwise under any patent or other rights of the SD Association or any third party. Nothing herein shall be construed as an obligation by the SD Association to disclose or distribute any technical information, know-how or other confidential information to any third party.

Specifications are subject to change without notice. Nonmetric weights and measurements are approximate. All data were deemed correct at time of creation. SD Association is not liable for errors or omissions. All brand, product, service names and logos are trademarks and/or registered trademarks of their respective owners and are hereby recognized and acknowledged.

Trademarks Notice:

SD logos and trademarks are owned and licensed by the SD-3C LLC.

PCI Express® is a registered trademark of PCI-SIG®.

NVM Express™ and NVMe™ are trademarks of NVM Express, Inc.

TCG Storage specifications are copyrighted and published by the Trusted Computing Group®.

The Trusted Computing Group mark is trademarked by Trusted Computing Group.

www.sdcard.org | ©2022 SD Association. All rights reserved

Executive Summary

Major market trends in memory technology and applications influence the evolution of SD and microSD memory cards. Ever-evolving memory technologies continuously increase the memory capacity of these tiny removable memory cards as well as improve their performance. The SD Express specification incrementally increased innovation by adding the PCIe and NVMe architectures to SD and microSD memory cards. SD Express memory cards now benefit from leading-edge and market-proven memory interfaces used by the most advanced system architectures found across various product categories in the market today.

SD Express opens new and evolving application opportunities and use cases for SD and microSD memory cards: Chromebooks (as its system memory or memory expansion), drones, surveillance cameras, dash cameras, gaming consoles, virtual reality (VR) headsets/glasses, small IoT modules and more.

SD memory cards have occasionally been used as a replacement for embedded memory since they offer easier maintenance and serviceability in the field. Typically, these cards serve as memory expansion to complement a relatively small embedded memory. The memory expansion by the SD memory card provides overall performance, both sequential and random, comparable to the device's embedded memory, thereby allowing applications or system files to be run from the card seamlessly.

SD Specification version 9.0, released in February 2022, introduces new features to further support products using conventional SD memory cards, as well as SD Express, in the use cases mentioned earlier. When using these features, the card is usually tightly bound to a specific host product, sometimes as semi-embedded where it is accessible under a cover with providing easy access for increased serviceability, maintainability and replaceability.

The new optional features found in Part 1 of the Physical Layer Specification V9.0 (SD9.0) are:

- **Boot –** Fast Boot and Secure Boot features give cards the ability to serve as a device's boot code memory by using a simple and easy fast boot code uploading process, along with secured methods of providing boot code updates
- **TCG Storage –** a secured storage method defined by the Trusted Computing Group adding a self-encrypted drive capability
- **RPMB –** Replay Protected Memory Block offers a secured hidden memory accessible only through a secured authentication process and provides a secured write-protect mechanism, secured boot code update and replay protection security mechanism

www.sdcard.org | ©2022 SD Association. All rights reserved

New Infrastructure Found In SD 9.0

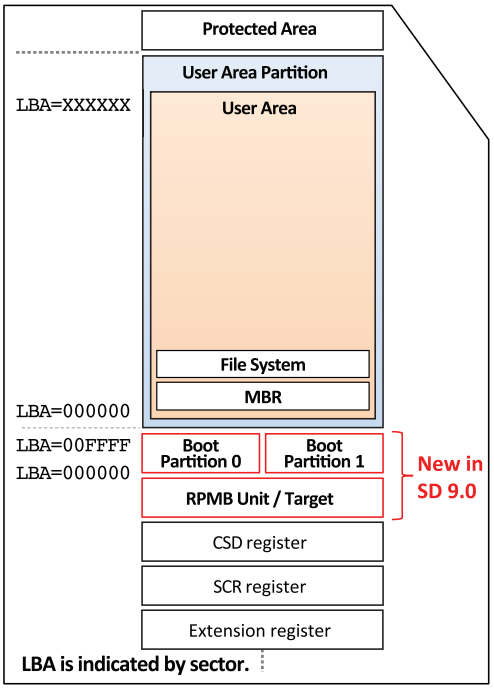


Figure 1-1
Newly added memory structure for Boot and RPMB

The new features added in SD 9.0 required new infrastructure for SD memory cards as follows.

- New internal memory structure for a card:
  - Two new partitions were added supporting the Boot function and described in greater detail in Section 3 below
  - RPMB Unit is a hidden memory area accessible in a secured manner

- Two new commands were added:
  - SECURE_RECEIVE (ACMD53)
  - SECURE_SEND (ACMD54)

These new pass-through commands allow a host to communicate with the card using various security protocols including TCG. ACMD53 and ACMD54 behave like Multiple Block RD/WR and have the following structure:

- Enhanced Write Protect: Write Protect Until Power Cycle is an additional Write Protect (WP) mode that was added as a WP state available only until a power cycle occurs and is supported only on an RPMB enabled card. The Initial State diagram shows possible transitions between the various WP modes. By using the Enabling procedure, RPMB allows users to use the optional Write Protect Until Power Cycle or Permanent Write Protect features.

Byte \ Bit	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 by T10 / INCITS)					
2	[31:24] Security Protocol Specific (15:8		) (as defined in TCG spec)					
3	[23:16] Security Protocol Specific (7:0)		(as defined in TCG spec)					
4	[15:8] Reserved							
5	[7:1] CRC7							[0] Stop Bit

Figure 1-2 SECURE_RECEIVE and SECURE_SEND Command Structure

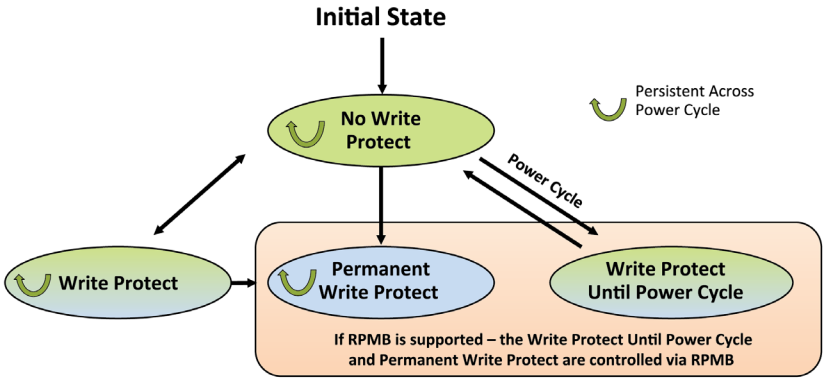


Figure 1-3 Possible transitions between Write Protect modes

www.sdcard.org | ©2022 SD Association. All rights reserved

Boot

Boot Concept

Boot function enables any device, especially IoT or mobile hosts, to store their boot code on the SD memory card. By using this feature, it is possible to minimize the size of non-volatile embedded memory for storing a primary bootloader by using the Unified Extensible Firmware Interface (UEFI) to manage secure boot. It also provides flexibility in implementing secure boot loader for any operating system. By storing codes with a specific signature that binds a specific host and a specific SD memory card, it prevents replacement of a semi-embedded card by third person.

It is important for these hosts to fetch their boot code promptly after power-up because they need to be activated as soon as possible. To achieve that requirement, Boot Partitions and Fast Boot are introduced as key functionalities of Boot.

Boot function is supported by any SD memory card, either through the SD protocol using the SD interface or through the NVMe protocol using the PCIe interface on SD Express cards. An exception is the fast boot operation, explained below, which may be implemented on the SD interface only.

When the card supports Boot function, it has exactly two Boot Partitions separate from the conventional User Area Partition. The host selects either one of the three partitions as a target partition by a specified command. The boot code is stored in the Boot Partitions that are activated earlier than the User Area. To secure the boot code, RPMB authentication is required before being activated, rather than writing data to the Boot Partition or erasing data in it. However, when reading from the Boot Partition, no authentication is necessary. Defining two Boot Partitions realizes *mirroring* by storing the identical boot code in both Boot Partitions and provides an *easy rollback* by setting aside a previous version of the code in either of these locations.

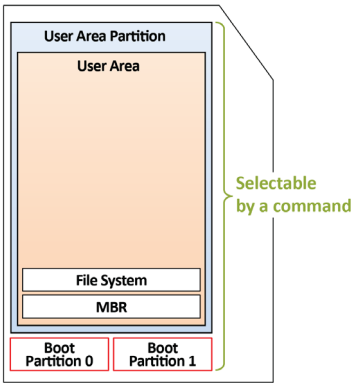


Figure 2-1: Boot Partitions and User Area Partition

Since SD memory cards are removable, the bus speed mode just after power-up is automatically set to the lowest one called 1-bit Default Speed mode that operates up to 3.1MB/s in order to establish the communication in any combinations between host and card. But this bus speed mode is too slow for practical use today. According to the conventional SD specification, several command transactions such as bus width changing, signal voltage switching, and multiple times of tuning operation, used for adjusting the data sampling point in the host, are required to utilize faster SD bus (e.g., UHS-I SDR104 mode, up to 104MB/s). But this process requires a comparatively large size boot loader for the initial host code for loading the boot code, and a longer time period to finish boot code loading. Since these traditional methods are not preferable for host design, Fast Boot for SD memory cards is introduced to reduce the size of the boot loader and for the duration of the booting process.

Starting Fast Boot is a simple host operation, much like driving the CMD line low for more than 74 clocks. By using this operation, the bus speed mode automatically switches to SDR104 as previously set in the card and it includes the tuning operations so the boot code is transmitted from the card to the host via the faster bus. Therefore, with SDR104 it takes just 0.3 seconds to transmit a 32MB boot code.

Boot function is also supported by NVMe except Fast Boot. Further detailed explanation about Boot over NVMe may be found in the NVM Express Base Specification.

www.sdcard.org | ©2022 SD Association. All rights reserved

Usage Examples

SD memory cards' long-standing advantage is letting customers select the right card to meet their desired use. The new Boot function is also helpful for many small, light and thin hosts. IoT or mobile hosts can especially benefit because storage media for both boot code and general data, like images or text, can be unified.

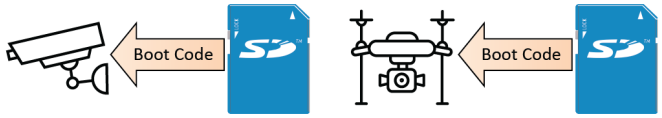
Here are some usage examples of Boot function over an SD memory card.

1. Security Camera

Security cameras have relied on SD memory cards as their primary storage device for many years. It is preferable to now merge the storage media for both boot code and video data to reduce memory costs. Occasionally, boot code for security cameras requires updating and some cameras are installed in poor radio communication environments, making it difficult to update boot code found on embedded storage over the air. Those situations require a special tool for updating the boot code. However, exchanging the card provides an easier upgrade when the camera obtains its boot code from the card.

2. Drone

Much like security cameras, it is very beneficial for a drone to simplify storage and shrink its overall weight and housing. Given their unique usage, there is always the possibility that embedded storage media may fail due to a crash. Embedded storage is hard, or even impossible to replace. But thanks to new boot functionality, drones that combine boot and image storage onto an SD memory card may be easily revived by replacing the damaged card equipped with boot code.



1. Security Camera **2. Drone**

Figure 2-2: Usage Examples

TCG Storage Security in SD Memory Cards

The Trusted Computing Group (TCG) provides open standards for secure computing, including enterprise storage and mobile devices, to name a few. Thousands of vendors offer a variety of TCG-based products, including hardware, applications and services. TCG was adopted in the market mainly for self-encrypted drive (SED) applications. The TCG Storage protocol was already defined to be used over NVMe and other various command layer protocols.

To introduce TCG security, while maintaining backward compatibility to the existing SD specifications, the following items are defined:

- **Protocols over SD interface for TCG security -** ACMD53 and ACMD54 correspond to IF-RECV and IF-SEND respectively and are defined in TCG Storage Architecture Core Specification

- **Specifications for realizing MBR Shadowing in SD memory cards -**
  The SD implementation of MBR Shadowing features are defined in the TCG Specification, along with the pre-boot authentication sequence, all are described in SD 9.0

TCG function may be supported by any SD, SD UHS-I or SD Express memory cards. TCG is not defined for UHS-II mode and cannot be implemented in UHS-II cards.

SD 9.0, along with the Extended Security Addendum v1.0, defines how TCG may be used on SD memory cards, either through the SD protocol using the SD interface or through the NVMe protocol using the PCIe interface on SD Express cards. The use of TCG through the NVMe interface is the same as defined in NVMe standards; therefore, existing drivers may be used.

www.sdcard.org | ©2022 SD Association. All rights reserved

TCG specifications define the Storage Interface Interaction Specification (SIIS) used with the SD protocol.

TCG Storage devices may be configured in various ways. The exact TCG for an SD memory card configuration may be found in the SD Extended Security Spec v1.0. Basically, it is a reduced version of OPAL 2.01 where only a single admin is supported versus four in OPAL.

TCG storage performs two major functions:

1. Encrypt/Decrypt Advanced Encryption Standard (AES) automatically any user data written/read to/from the user area of the card
2. May Lock/Unlock access to the user area of the card

It serves as access protection if the user area access is locked or as data protection, if the storage media is removed from the host.

Further detailed explanation about TCG and its usage as SED with NVMe may be found in the following link.

Replay Protected Memory Block (RPMB)

RPMB is introduced to store data in an authenticated memory area for the purpose of protecting data from a replay attack or avoiding unexpected data updates.

The RPMB feature may be supported through the standard SD interface. For an SD Express memory card, RPMB is available through both the SD and PCIe interfaces. The usage of RPMB through PCIe interface is done through the NVMe protocol.

Note that this function is not defined for UHS-II mode and cannot be implemented for UHS-II cards.

An authentication key must be stored in a secured environment that typically occurs during the manufacturing process. This creates a shared secret with the host application. Therefore, RPMB is best when an OEM uses specific cards with specific hosts.

An RMPB enabled card may have a Secured Write Protect capability. RMPB restricts the use of the Write Protect features – setting to Permanent Write Protect or Write Protect Until Power Cycle, that occurs after performing the enabling procedure by using RPMB authentication.

The enabling procedure also provides secured access to the boot partitions for updating or erasing the boot code saved in either of the two boot partitions.

Usage Examples

1. **Software Version Authentication to Prevent a Downgrade Attack**
   Software using RPMB to protect itself from a downgrade attack would check for a new, updated version number during the upgrade procedure. If the *new version* number is lower than the one already present in RPMB, the installer would reject the supposed update. Due to the nature of RPMB, there is no way for an attacker to change the software version information stored in the RPMB, because it requires access to the secret key.
2. **Secure Boot**
   Prevention of undesired, or hacked, code from running on a device starts with an assurance that the very first piece of code that the processor reads and executes from the storage device is legitimate. This initial code, the bootloader, is located on the SD boot partition and must be write-protected from malware modification. Every change to the boot partition requires the enabling procedure by using RPMB authentication. The secured write-protect mechanism is primarily used to protect the boot code or other sensitive data on the card from changes or deletion by unauthorized applications.

Further explanation about RPMB and its usage may be found in this whitepaper*.

* Note: Published by Western Digital and focused on eMMC; however, the RPMB concepts are relevant for SD and NVMe protocols.

www.sdcard.org | ©2022 SD Association. All rights reserved