SD Association

# Introduction to SD Specification 9.0

## Public Webinar

September 2022

# Disclaimers and Trademarks

SD Association

## Forward-Looking Statements

During our webinar today we will be making forward-looking statements. Any statement that refers to expectations, projections or other characterizations of future events or circumstances is a forward-looking statement, including those relating to industry trends, standardization plans and any SD Association's related plans. Actual results may differ materially from those expressed in these forward-looking statements due to various factors. We undertake no obligation to realize these forward-looking statements, which speak only as of the date hereof.

## Trademarks

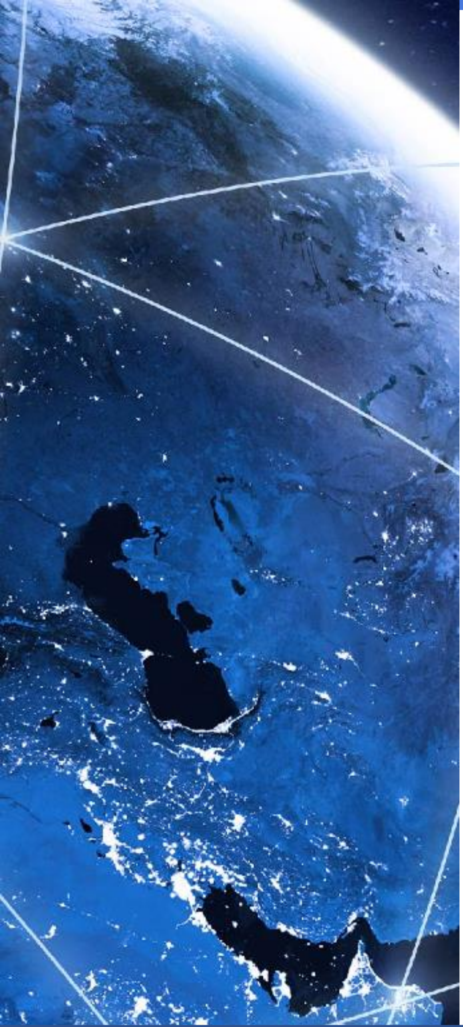
SD and related marks and logos are trademarks of SD-3C LLC. © 2019-2022 SD-3C LLC. All Rights Reserved.

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

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

# Agenda

- □ **Introduction - Yosi Pinto,** Chairman and Technical Committee Chair
- □ **Boot Functions  - Tadashi Ono,** UHS TG Co-Chair / Panasonic Connect Co., Ltd
- □ **TCG and RPMB Functions - Yoni Shternhell,** Advanced Security Chair / SanDisk LLC



# Introduction to SD Spec. 9.0

SanDisk

## Introduction

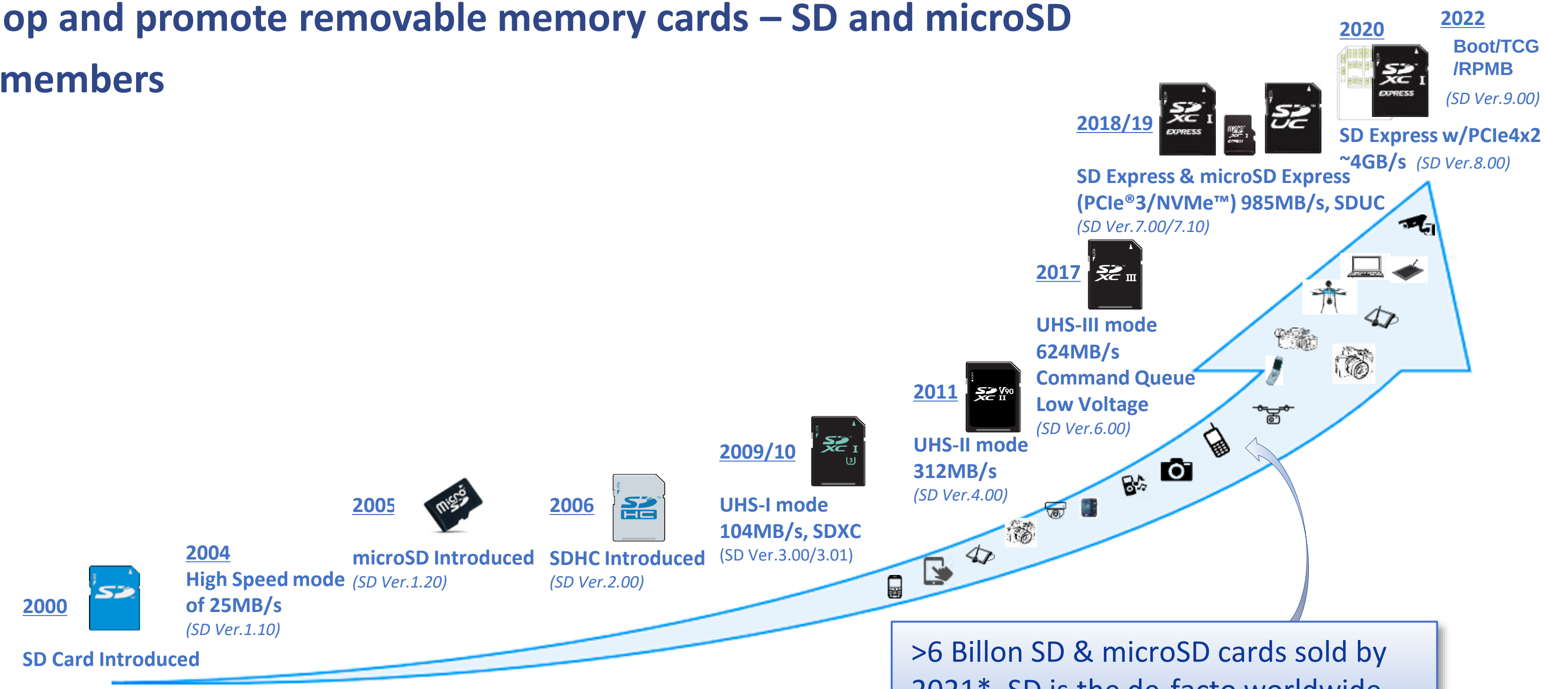
***Yosi Pinto, Chairman and Technical Committee Chair, SD Association***

*Senior Technologist at Technology & Strategy Division in Western Digital (formerly SanDisk) and Chairman of the Board and the Technical Committee chair at the SD Association.*

# SD Card Specifications Evolution

SD Association

- □ **SD Association was formed in 2000**
- □ **Develop and promote removable memory cards – SD and microSD**
- □ **~780 members**



**2000**
**SD Card Introduced**

**2004**
**High Speed mode of 25MB/s**
*(SD Ver.1.10)*

**2005**
**microSD Introduced**
*(SD Ver.1.20)*

**2006**
**SDHC Introduced**
*(SD Ver.2.00)*

**2009/10**
**UHS-I mode 104MB/s, SDXC**
(SD Ver.3.00/3.01)

**2011**
**UHS-II mode 312MB/s**
*(SD Ver.4.00)*

**2017**
**UHS-III mode**
**624MB/s**
**Command Queue**
**Low Voltage**
*(SD Ver.6.00)*

**2018/19**
**SD Express & microSD Express (PCIe®3/NVMe™) 985MB/s, SDUC**
*(SD Ver.7.00/7.10)*

**2020**
**SD Express w/PCIe4x2 ~4GB/s** *(SD Ver.8.00)*

**2022**
**Boot/TCG /RPMB**
*(SD Ver.9.00)*

>6 Billon SD & microSD cards sold by 2021*. SD is the de-facto worldwide removable memory card standard

**To join: https://www.sdcard.org/join/**

* Source: Estimation using news published by SanDisk in 2015 ("2 Billion microSD cards sold by 2015") + TrendForce's report from 2019 ("total of ~3 billion cards sold within 2016-2019") and report from Futuresource of total of ~1M sold between 2020-2021

# Background

- □ **SD Express opens new opportunities and use cases for SD and microSD memory cards. Some of the potential usage:**
  - 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

Right To Repair

- □ **The Right-to-Repair legislation in EU and other areas – demands new serviceability requirements. Storage is one of the targeted components.**
- □ **SD cards may replace embedded devices in small systems (i.e. IoT, Drones) and SD Express enhanced this opportunity for devices that needs higher speed memory. Such usage of SD as semi-embedded memory may allow:**
  - Reduced memory components
  - Easy memory upgrade and improved serviceability options

# SD9.0 – What does it include?

SD Association

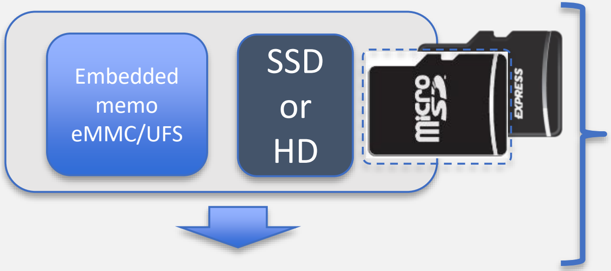
- □ **Part 1 v9.0 (SD9.0) adds new features to the SD standard:**
  - Boot
    - Fast Boot and Secure Boot features give cards the ability to serve as a device’s boot code memory by using a simple and easy fast boot code uploading process, along with secured methods of providing boot code updates
  - TCG Storage
    - A secured storage method defined by the **Trusted Computing Group** adding a self-encrypted drive capability
  - Replay Protected Memory Block (RPMB)
    - 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
- □ **SD9.0 features provide enhanced features that may open new opportunities for SD cards usually tightly bound to a specific host product as:**
  - Semi-embedded devices replacing the soldered embedded memory (IoT, Chromebooks, etc.)
  - As a secured memory for OEM applications (i.e. Gaming, Automotive, VR, etc.)

# SD Cards as Semi-Embedded Solutions

## □ Embedded memory vs Removable memory in current and future market

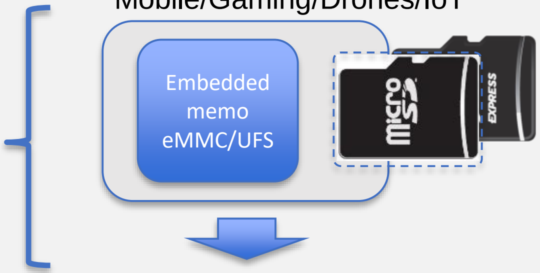
### Present

Mobile Computing and Automotive



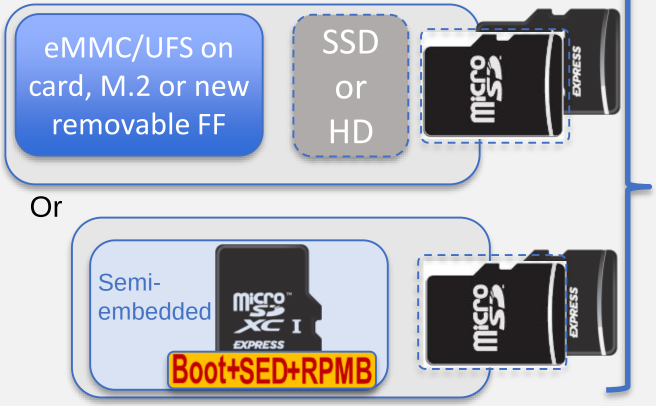
- Fast embedded mem for OS with enhanced security functions (boot, TCG, RPMB)
- Slow removable for off-line storage
- Optional fast Removable for App running and real-time rec/view (real mem expansion)
- No easy serviceability of embedded mem

Other Small Devices
Mobile/Gaming/Drones/IoT

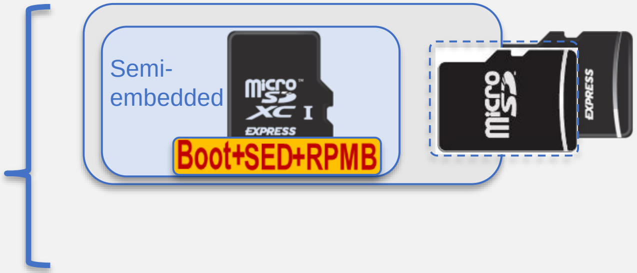


### Future

Future small/low cost Mobile Computing or for better Serviceability



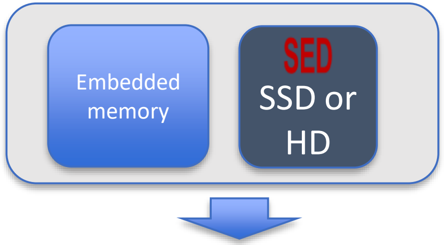
- Same, but with enhanced serviceability for embedded mem
- **Solution based on SD card may provide the same features [including Boot, Self Encrypted Drive(using TCG) and RPPB security] with reduced size and fewer components**



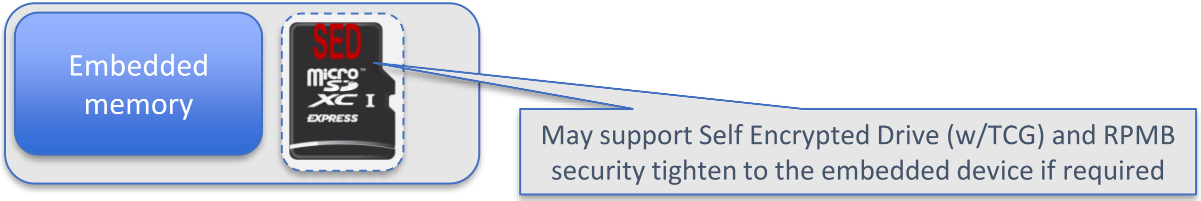
# SD Cards as OEM Cards Tightly Bound to Specific Hosts

- □ **Chromebooks, Gaming products, VR goggles, Automotive Infotainment Cards (i.e. Maps or Apps), IoT… to name a few**
- □ **May enjoy cards supplied by the product manufacturers or its contractors dedicated to being run on specific hosts**

Mobile Computing

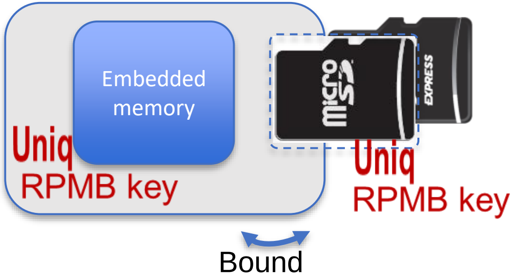


The main storage device (SSD or HD) may be replaced with SD Express in small low/cost systems



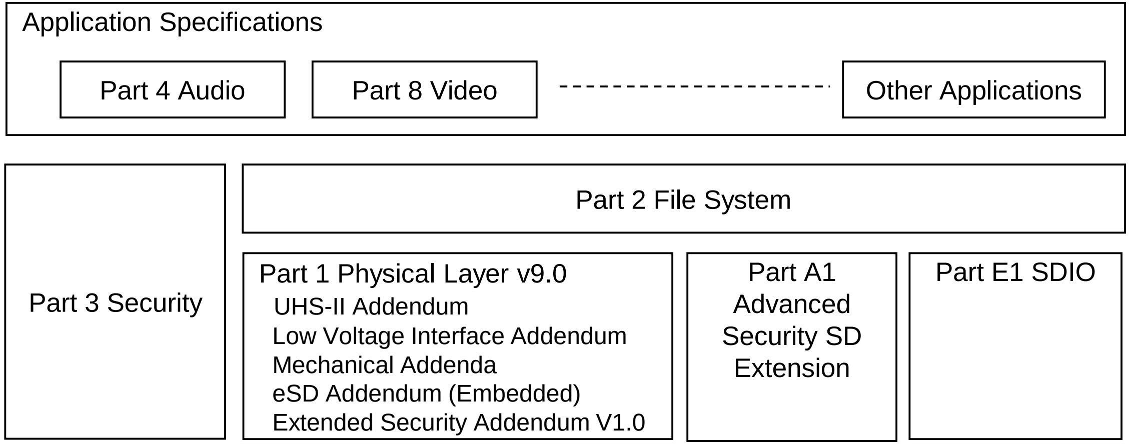
May support Self Encrypted Drive (w/TCG) and RPMB security tighten to the embedded device if required

Other Small Devices
Gaming/IR/Auto etc.



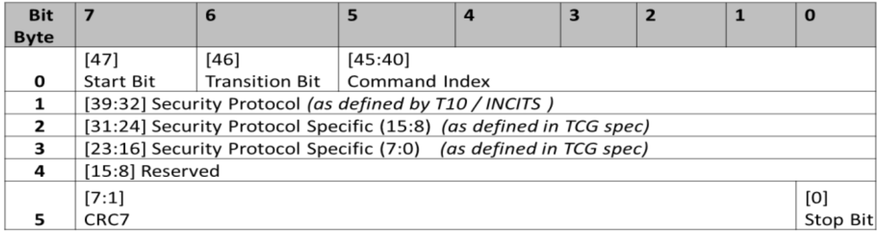
# SD9.0  Specification

- □ **SD9.0 Specification was introduced with:**
  - SD Specification Part 1  V9.0
  - Extended Security Addendum

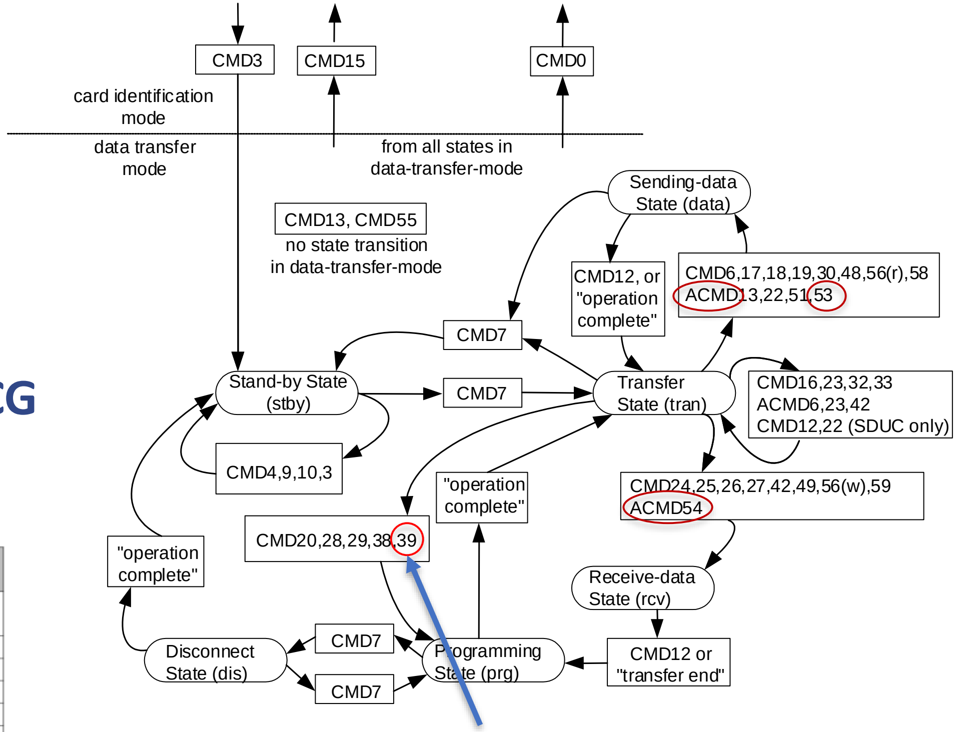

Application Specifications
Part 4 Audio
Part 8 Video
Other Applications
Part 3 Security
Part 2 File System
Part 1 Physical Layer v9.0
UHS-II Addendum
Low Voltage Interface Addendum
Mechanical Addenda
eSD Addendum (Embedded)
Extended Security Addendum V1.0
Part A1 Advanced Security SD Extension
Part E1 SDIO

# SD 9.0 : New Infrastructure

- □ **Two New Security Commands:**
  - – SECURE_READ – ACMD53
  - – SECURE_WRITE – ACMD54
- □ **Behave like Multiple Block RD/WR**
- □ **Allow a host to communicate with the card as pass-through command for various security protocols including TCG**
- □ **Have the following structure:**



| Bit<br>Byte | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
|---|---|---|---|---|---|---|---|---|
| 0 | [47]<br>Start Bit | [46]<br>Transition Bit | [45:40]<br>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]<br>CRC7 | | | | | | | [0]<br>Stop Bit |



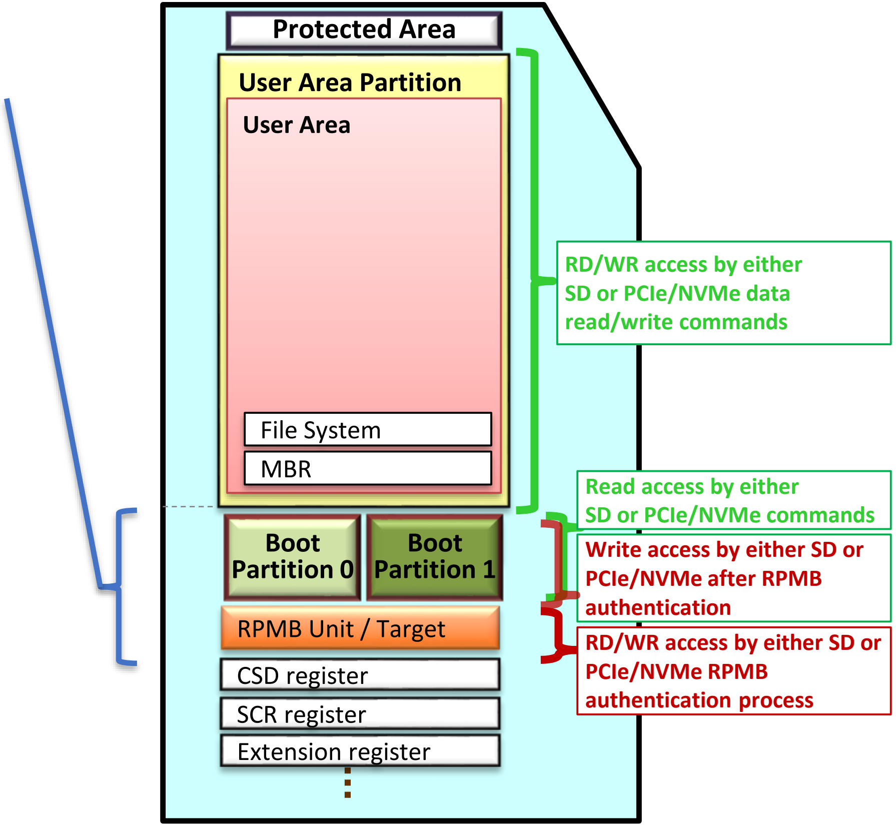
**SELECT_CARD_PARTITION (see next page)**

# SD 9.0 : New Infrastructure (cont.)

SD Association

## □ Three memory units were added:

- Two Boot partitions
  - Supporting the Boot function
  - CMD39 (New) is used to switch between the two partitions
- One RPMB hidden unit
  - A hidden memory area accessible in a secured manner



Protected Area
User Area Partition
User Area
File System
MBR
Boot Partition 0
Boot Partition 1
RPMB Unit / Target
CSD register
SCR register
Extension register
RD/WR access by either SD or PCIe/NVMe data read/write commands
Read access by either SD or PCIe/NVMe commands
Write access by either SD or PCIe/NVMe after RPMB authentication
RD/WR access by either SD or PCIe/NVMe RPMB authentication process

# Introduction to SD Spec. 9.0

Panasonic

## Boot Functions

***Tadashi Ono, UHS TG Co-Chair, SD Association***

*Supervisor at Advanced Research Lab. in Panasonic Connect Co., Ltd., and co-chair of the UHS TG for the SD Association.*

# Agenda

- □ **Introduction**
- □ **Application Examples**
- □ **Boot Functions**
  - – Function 1: Boot Partitions
  - – Function 2: Fast Boot
  - – Function 3: Boot Partition Protection by RPMB
- □ **Summary**

# Introduction

SD Association

□ **One of new features of SD9.0 is “Boot”, which can minimize the size of non-volatile memory in the host for storing its primary bootloader.**

– It is especially useful for IoT or mobile equipment.

□ **The following functions are newly introduced from SD9.0.**

1. Boot Partitions
2. Fast Boot
3. Boot Partition Protection by RPMB

□ **These functions are available over not only SD bus but also PCIe bus for SD Express card.**

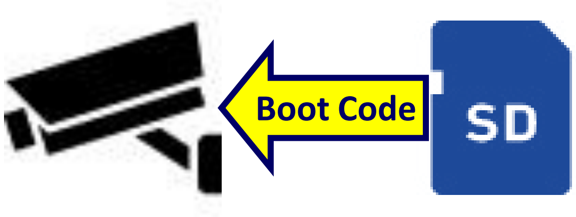
– Note: Fast Boot is introduced for SD bus only.

# Application Examples

SD Association

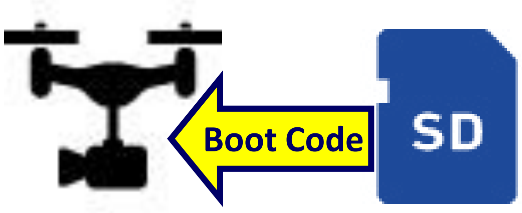
□ **Security Camera**

- Requirement for merging storage for both boot code and video data to reduce cost.
- Easy to update the boot code even in poor radio communication environment.



□ **Drone**

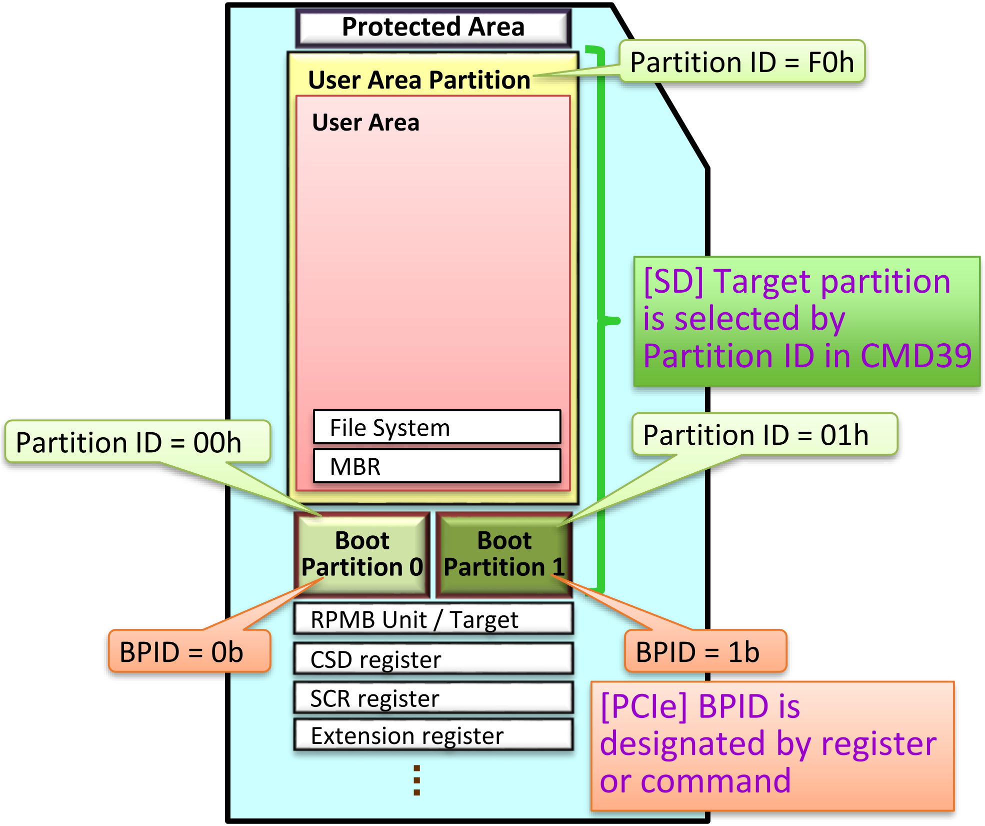
- Beneficial to simplify storage and shrink its overall weight and housing.
- Easily revive the boot code by replacing SD card even in a crash.



# Function 1: Boot Partitions

- □ **SD Card supporting Boot has**
  - – 1 User Area Partition, and
  - – 2 Boot Partitions (Boot Partition 0/1).

- □ **These partitions are accessible by both SD bus and PCIe bus**
  - – For SD bus, host issues CMD39 with the selected Partition ID as its argument.
  - – For PCIe bus, host designates BPID in BPRSEL register (read) or Firmware Commit Command (write) when accessing to Boot Partitions.



# Function 2: Fast Boot – Background

SD Association

- □ **Host requires boot code transmission immediately after power up with minimum operations.**

- □ **Just after power up, maximum speed of the SD bus is 3.1MB/s as a default.**
  - In order to establish the communication in any combinations between host and card.

- □ **However, it is too slow for boot code transmission today.**

- □ **Therefore, the Fast Boot function is introduced to enable transmitting boot code up to 104MB/s (SDR104 bus) in SD card.**

Note again: Fast Boot is supported only through SD bus.

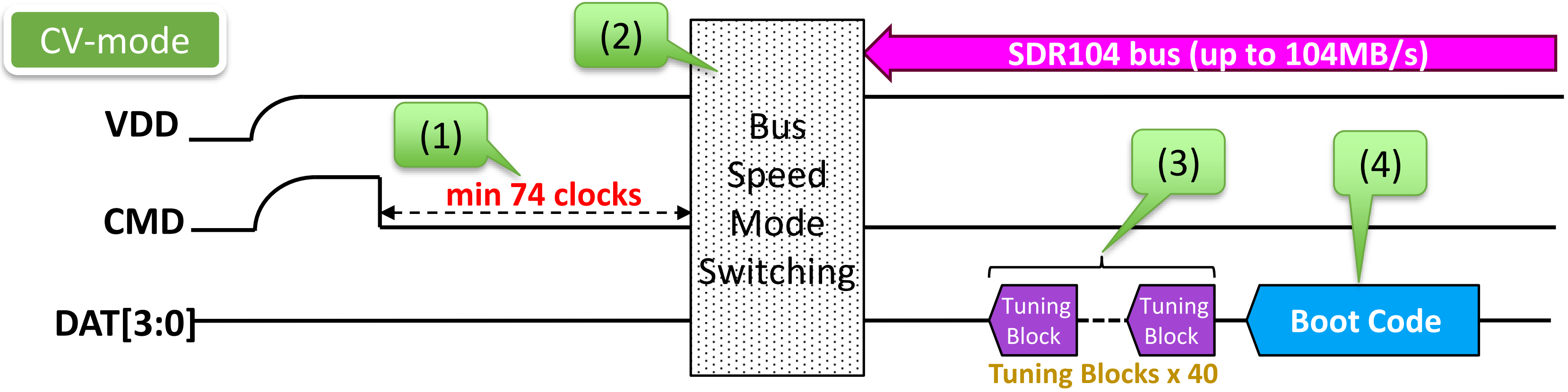
# Function 2: Fast Boot – Implementation to the SD Card

SD Association

- □ **Signal voltage shall be 1.8V in SDR104 bus.**
  - Default signal voltage of SD card is 3.3V.
- □ **In order that host detects appropriate signal sampling points, tuning process is required.**
  - Unlike UHS-I, tuning blocks are automatically transmitted from card to host without CMD19 to simplify the sequence.
- □ **The following two processing modes are introduced to the Fast Boot.**
  - Card that supports Boot shall implement both modes.
  - Host can choose either of them for performing Fast Boot.

| Mode | Trigger by the Host | Note |
|---|---|---|
| CV-mode | Driving CMD line Low | Standing for "CMD line Voltage" |
| CA-mode | Issuing CMD0 with a special argument | Standing for "CMD0 Argument" |

# Function 2: Fast Boot – CV-mode



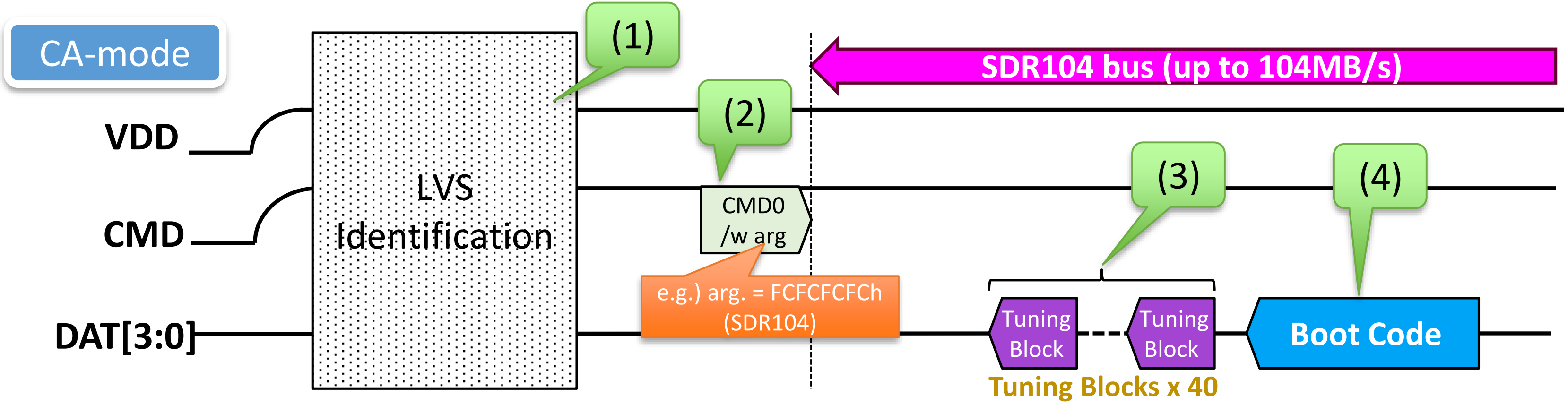
(1) Host starts CV-mode Fast Boot by driving CMD line low for at least 74 clocks.

(2) Bus speed mode switches to SDR104 (signal voltage to 1.8V etc.) to realize 104MB/s code transmission.

(3) Card repeats sending 40 tuning blocks for the tuning process by the host.

(4) After completing the tuning blocks transmission, card sends a boot code.

# Function 2: Fast Boot – CA-mode



(1) Host executes LVS identification to initialize card by 1.8V signaling.

(2) Host starts CA-mode Fast Boot by issuing CMD0 with an argument indicating bus mode.

- Argument “FCFCFCFCh” means SDR104 bus.

(3) Card repeats sending 40 tuning blocks for the tuning process by the host.

(4) After completing the tuning blocks transmission, card sends a boot code.

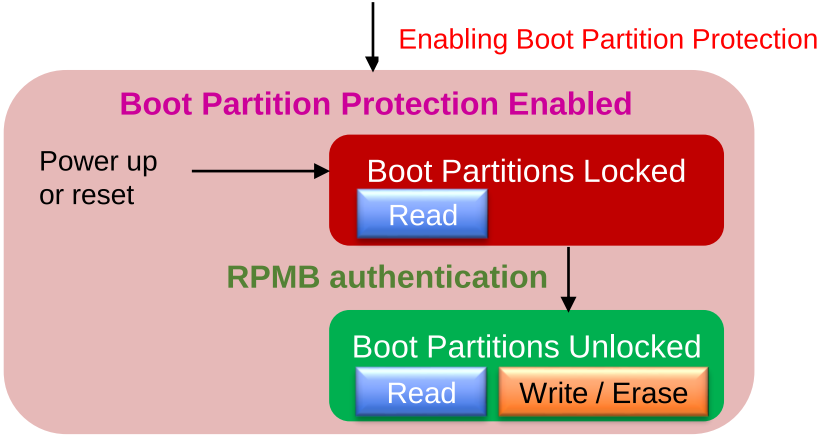
} Same as CV mode

# Function 3: Boot Partition Protection by RPMB

□ **Once boot code is written, Boot Partition Protection should be enabled for its security. At this time, Boot Partitions are locked after power up or reset.**

□ **After unlocking by RPMB authentication, write and erase operations for the Boot Partitions become possible.**

□ **Read operation for them is always allowed.**



# Summary

SD Association

□ **Boot functions are defined for unifying the storage for boot code and user data.**

- It is expected for host to store both kinds of data in one SD card.

□ **Fast Boot provides high-speed and immediate boot code transmission after power up.**

- Two sequences are introduced on SD bus with minimum host operations.
- Tuning process is modified in order to make issuing commands unnecessary.

□ **Boot Partition Protection is also available for providing security of boot code.**

# Introduction to SD Spec. 9.0

## TCG and RPMB Functions

***Yoni Shternhell, Advanced Security Chair, SD Association***

*Technologist at Memory Technology Division in Western Digital (formerly SanDisk) and Application WG chair and the Advanced Security WG chair at the SD Association.*

# TCG Storage Security in SD Cards

- □ **TCG Storage WG develops standards for secure computing, including client, datacenters and enterprise storage, mobile devices, gaming and more**
- □ **TCG Storage WG Opal family includes Opal, Opalite, Ruby and Pyrite SSCs**
- □ **TCG Storage protocol can be used over NVMe and other command layer protocols**
- □ **TCG interactions with other protocols are defined in the Storage Interface Interaction Specification (SIIS) (soon to be approved document)**
- □ **The new TCG functionality in SD Cards:**
  - Support of Ruby SSC – which is in practice an OPAL 2.01 with the more flexible requirements
  - Enables a Self Encrypted Drive capability
  - Use the newly defined commands SECURE_READ (ACMD53) and SECURE_WRITE (ACMD54) to correspond to IF-RECV and IF-SEND
  - Enables the TCG MBR Shadowing capability
- □ **TCG is supported by any SD card through the SD interface or PCIe/NVMe interface (in SD Express cards). It is not supported in SD-UHS-II cards**

# TCG Self-Encrypting Drive (SED)

( as defined by TCG Standard)

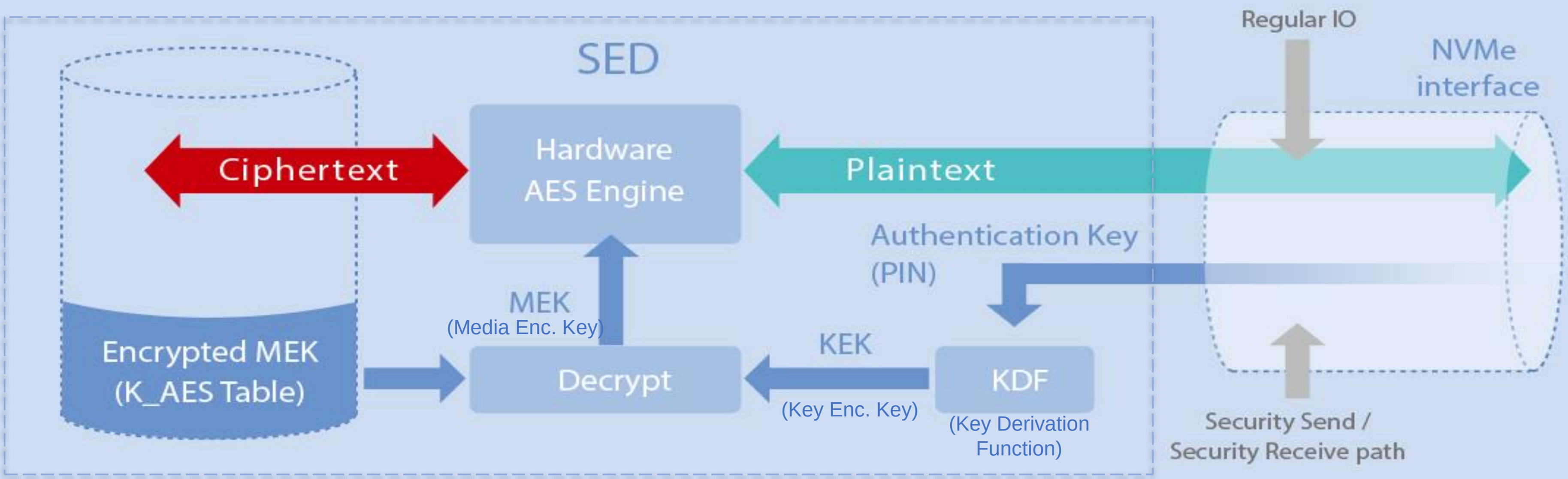
SD Association

- □ **A SED is a Storage Device that integrates encryption of user data at rest**
- □ **All user data written to the Storage Device is** *encrypted* **by specialized hardware implemented inside the Storage Device Controller**
- □ **The user data is** *decrypted* **as it is read**
- □ **The** *encryption* **and** *decryption* **are performed using a Media Encryption Key (MEK) generated internally inside the SSD or the SD Card**
- □ **TCG Opal Family specs defines a management interface for a host application to activate, provision, and manage encryption of user data**
- □ **It also provides a mechanism by which an Authentication Credential can be set by a host application that manages the TCG functionality in the drive, in order to enable control of access to the user data.**

# How Does the Crypto Work?

( as defined by TCG Standard)

- □ **When an Authentication Credential (PIN) has been set and the device is *locked*, it is no longer possible to access the user data**
- □ **Once the correct Authentication Credential has been supplied to the Storage Device by the host, and the Storage Device is *unlocked*, data can be read from and written to the device once again**

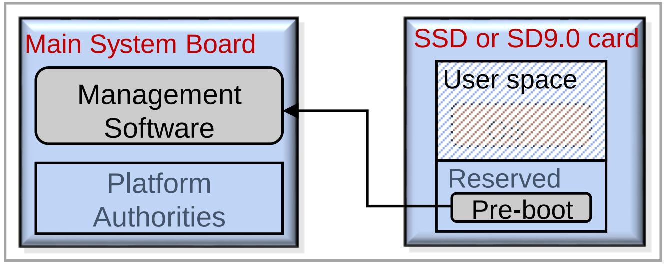


# Master Boot Record (MBR) Shadowing

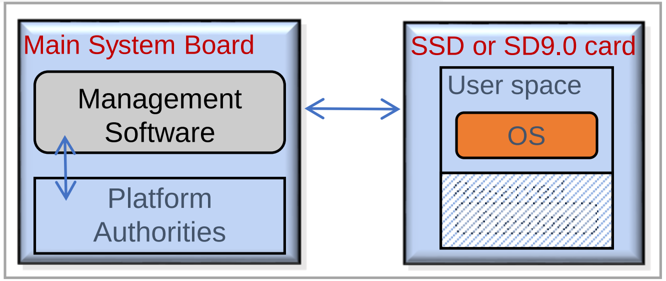
- □ MBR Shadowing provides a way to boot from a drive that is encrypted and locked
- □ Contains an ISV's pre-boot authentication (PBA) code, and this "shadow" is loaded and executed by the host PC at power-on
- □ The PBA code is completely independent of the system's main OS and the BIOS

Notebook / PC

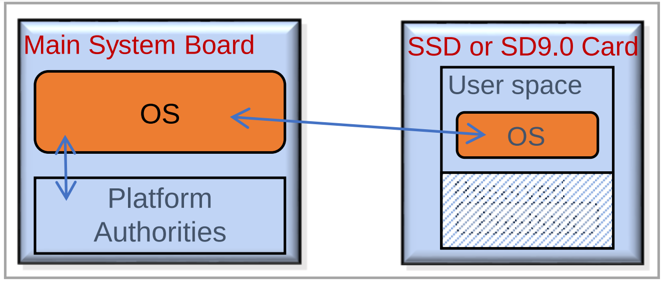
- □ **Initial Power-up**
  - □ When the system first requests for data, the drive returns the pre-boot code (MBR shadow).



- □ **Authentication and Unlock**
  - □ The pre-boot code manages the authentication process with both internal and external authorities.
  - □ After the appropriate authentications, the management software unlocks the regular user space.



- □ **Resume Normal Boot**
  - □ After the drive is unlocked, the management software sends the system back to the boot process.
  - □ The system's request for the MBR now returns the true MBR and the OS is loaded completing the boot process.



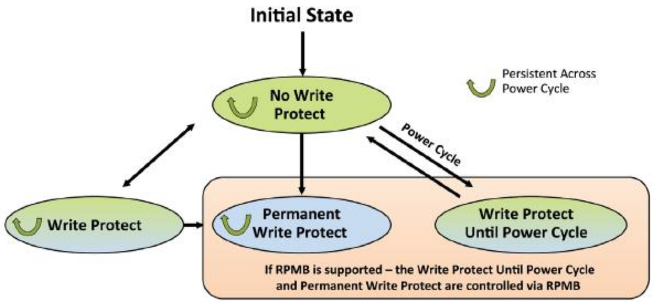
# Replay Protected Memory Block (RPMB)

- □ **RPMB stores data in an authenticated hidden memory area for the purpose of protecting data from a replay attack or avoiding unexpected data updates**
- □ **Enables protection for write-protect mechanism and secured boot code update**
- □ **Can only be read and written via successfully authenticated read and write accesses**
- □ **The data may be overwritten by the host, but can never be erased**
- □ **Prevents illegal data access or copy with a Security Key (SHA-256)**

# Replay Protected Memory Block (RPMB)(Cont.)

## □ Enhanced Write Protection for RPMB Enabled Card

- Write Protect Until Power Cycle is newly defined in CSD Register
- RPMB Enabled Card requires secured procedure to transit either of write protection states:
  - Permanent Write Protect
  - Write Protect Until Power Cycle
- The secured procedure consists of three steps:
  1) Execute RPMB authentication to access RPMB target
  2) By enabling write protection control in RPMB target, the two write protection bits in CSD Register can be set
  3) Setting either write protection bit in CSD Register makes the transition to one of the write protection states



Initial State

No Write Protect

Persistent Across Power Cycle

Power Cycle

Write Protect

Permanent Write Protect

Write Protect Until Power Cycle

If RPMB is supported – the Write Protect Until Power Cycle and Permanent Write Protect are controlled via RPMB

# RPMB Usage Examples

## □ Software Version Authentication to Prevent a Downgrade Attack

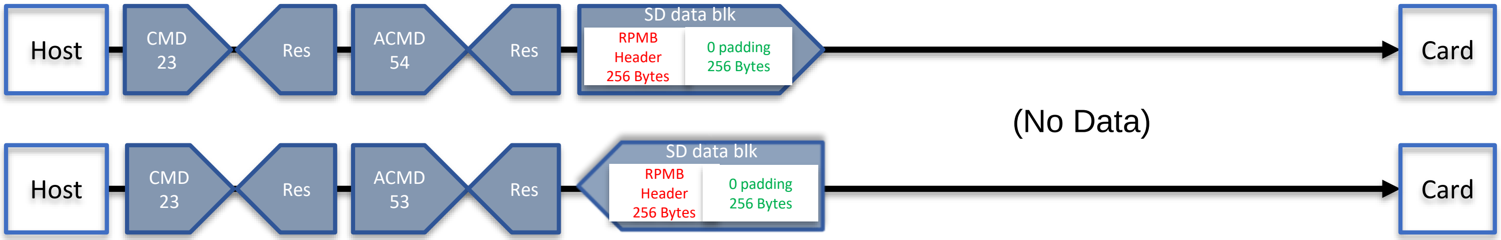
Software using RPMB to protect itself from a downgrade attack would check for a new, updated version number during the upgrade procedure. If the *new version* number is lower than the one already present in RPMB, the installer would reject the supposed update. Due to the nature of RPMB, there is no way for an attacker to change the software version information stored in the RPMB, because it requires access to the secret key.

## □ Secure Boot

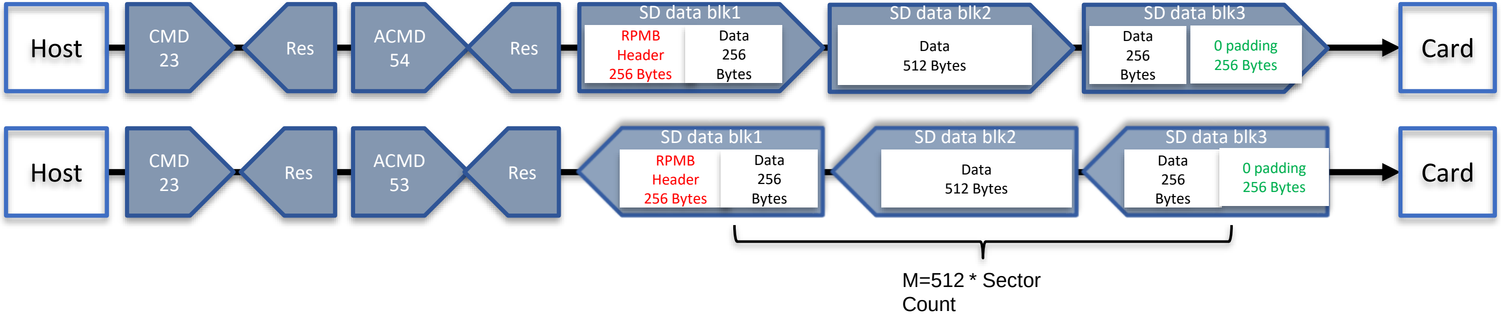
Prevention of undesired, or hacked, code from running on a device starts with an assurance that the very first piece of code that the processor reads and executes from the storage device is legitimate. This initial code, the bootloader, is located on the SD boot partition and must be write-protected 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.

# SD9.0 RPMB Payload

## Without Data Transfer



## With Data Transfer



# T10 SPC-6

- □ T10 is a Technical Committee in INCITS (International Committee for Information Technology Standards)
- □ Responsible to standardize the SCSI Primary Commands - 6 (SPC-6)
  - One related topic it defines is the Security Protocol Code IDs for all transport
- □ A new and published SPC-6 version now includes the new Security Protocol code assigned to SD Association (E7h)
- □ The new Security Protocol (E7h) field used for TCG/RPMB in ACMD53/54

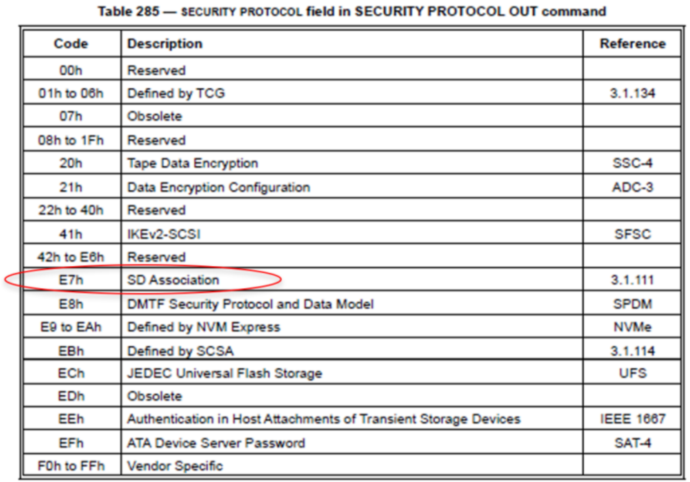


Table 285 — SECURITY PROTOCOL field in SECURITY PROTOCOL OUT command

| Code | Description | Reference |
|---|---|---|
| 00h | Reserved | |
| 01h to 06h | Defined by TCG | 3.1.134 |
| 07h | Obsolete | |
| 08h to 1Fh | Reserved | |
| 20h | Tape Data Encryption | SSC-4 |
| 21h | Data Encryption Configuration | ADC-3 |
| 22h to 40h | Reserved | |
| 41h | IKEv2-SCSI | SFSC |
| 42h to E6h | Reserved | |
| E7h | SD Association | 3.1.111 |
| E8h | DMTF Security Protocol and Data Model | SPDM |
| E9 to EAh | Defined by NVM Express | NVMe |
| EBh | Defined by SCSA | 3.1.114 |
| ECh | JEDEC Universal Flash Storage | UFS |
| EDh | Obsolete | |
| EEh | Authentication in Host Attachments of Transient Storage Devices | IEEE 1667 |
| EFh | ATA Device Server Password | SAT-4 |
| F0h to FFh | Vendor Specific | |

# Thank you for attending!