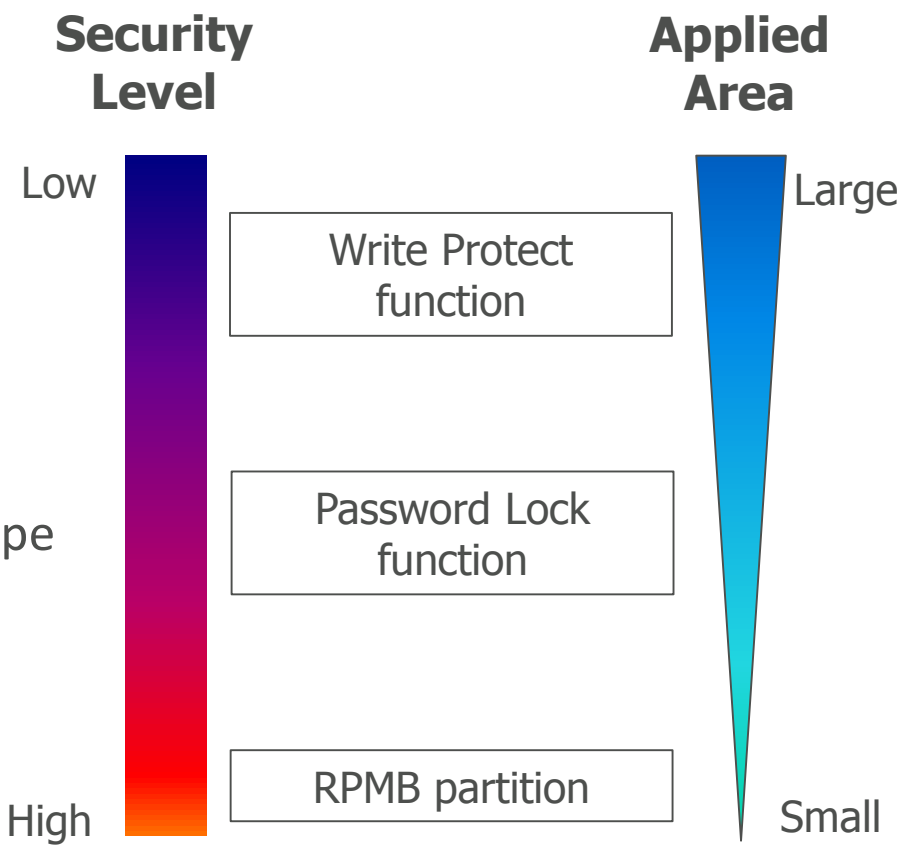
eMMC Security Features

Protection & Security

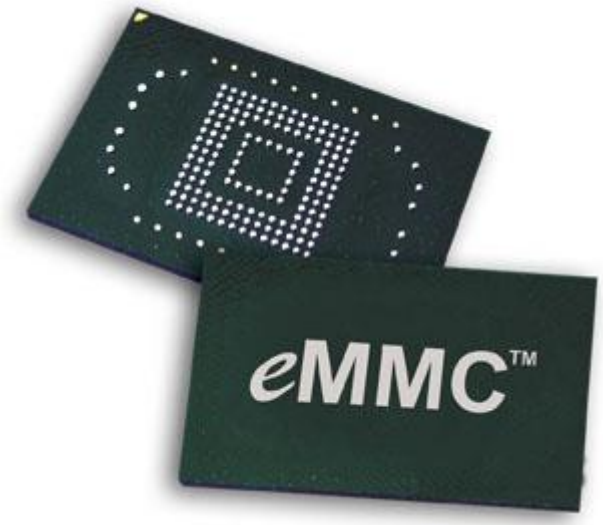
Multiple layers of data protection and security exist for eMMC devices including:

- Ball Grid Array (BGA)
- Write Protection
- Password Lock
- Replay Protected Memory Block (RPMB)
- New from 4.51 and 5.0 Sanitize and Secure removal type



Ball Grid Array (BGA)

- The first level of protection for eMMC is its package.
- Once the BGA package is soldered on the board, signals
- cannot be probed.
- The suggestion is use blind vias under BGA packages to hide trace.



Write Protection

- eMMC offers **write protection** to prevent data corruption at power-on and malicious write or read-only coverage over a selectable area
- Write protection can be enabled on a small area of a partition or over the entire device with three different types:
  - Permanent - Does not allow host to disable the write protection on the selected area once set
  - Temporary - Area protected can be unprotected by various methods
  - Power-on - Protected area selected can be unprotected by power cycle or hardware reset (Rst_N)

It is suggested that any write protect disable bits be set if no WP is to take place to avoid malicious or accidental setting of write protection

Write Protection

CSD ENABLED

CSD enabled write protection is enabled by programming bits in the CSD (cmd27)

Permanent (CSD[13])
Temporary (CSD[12])

Device Partitions

Extended CSD ENABLED

Permanent (eCSD[173])
Power-on (eCSD[173])
Temporary (default)

Permanent (eCSD[171])
Power-on (eCSD[171])
Temporary (default)

Permanent (eCSD[171])
Power-on (eCSD[171])
Temporary (default)
(Lock/Unlock)

eCSD enabled write protection is enabled first by programming bits in the eCSD (cmd6) then setting write protect group sized areas utilizing cmd28, cmd29, cmd30, and cmd31

Permanent Write Protect

When enabled, areas with permanent write protection are treated as read-only and protection cannot be removed

CSD Register (cmd27)

- Coverage: All areas of device (simultaneously)
- Enable: Set PERM_WRITE_PROTECT byte (CSD[13]) to 1
- Exceptions:
  - If eCSD byte USER_WP bit CD_PERM_WP_DIS (eCSD[171:6]) is enabled, setting CSD[13] cannot be enabled
  - If any area of device is already set as another type of write protect (temporary, power-on) the protection type will be over-ridden and will become permanently protected;
  - Permanent WP cannot be over ridden by another write protect type

Permanent Write Protect

Extended CSD Register (cmd6)

- Coverage: Boot, User, & General Area Partitions (selectively)
- Enable User/GPP:
  - Set eCSD byte USER_WP bit US_PERM_WP_EN (eCSD[171:2])
  - Issue command cmd28 for desired write protect group
  - Once set by SET_WRITE_PROT (cmd28) the area cannot be unprotected
- Exceptions:
  - If eCSD byte USER_WP bit US_PERM_WP_DIS (eCSD[171:4]) is enabled, US_PERM_WP_EN eCSD[171:2] cannot be enabled
  - Permanent write protection cannot be over ridden by another write protect type

Permanent Write Protect

Extended CSD Register (continued)

- Enable Boot:
  - Set eCSD byte BOOT_WP bit B_PERM_WP_EN (eCSD[173:2])
  - Once set by SET_WRITE_PROT (cmd28) the area cannot be unprotected
- Exceptions:
  - In some instances, the boot partition is the same size or smaller than a write protect group and protecting any sector within the boot partition so will permanently protect the entire boot partition.
  - Permanent write protection cannot be over ridden by another write protect type
  - If eCSD byte BOOT_WP bit B_PERM_WP_DIS (eCSD[173:4]) is enabled, B_PERM_WP_EN eCSD[171:2] cannot be enabled

Temporary Write Protect

When enabled, areas with temporary write protection are treated as read-only but protection can be removed

CSD Register (cmd27)

- Coverage: Boot, RPMB, and all User & General Areas
- Enable:
  - Set TMP_WRITE_PROTECT byte (CSD[12]) to 1
- Exceptions:
  - If CSD byte PERM_WRITE_PROTECT (CSD[13]) is enabled, setting byte CSD[12] is ignored
  - If any area of device is already set as another type of write protect (permanent, power-on) the protection type will NOT be overridden upon enabling TMP_WRITE_PROTECT

Temporary Write Protect

Extended CSD Register (cmd6)

- Coverage: Boot, User, & General Area Partitions (no RPMB)
- Enable:
  - If no other write protection features are set, Boot, User, and GPP areas are designated as temporary write protect by default; issue cmd28 for desired write protect group
- Exceptions:
  - If a desired area is already set as another type of write protection (permanent or power-on) it cannot be overridden as temporary
  - In some instances, the boot partition is the same size or smaller than a write protect group and protecting any sector within the boot partition so will protect the entire boot partition

Power-on Write Protect

Areas with power-on write protection are read-only until protection is removed with power cycle or hardware reset

Extended CSD Register (cmd6)

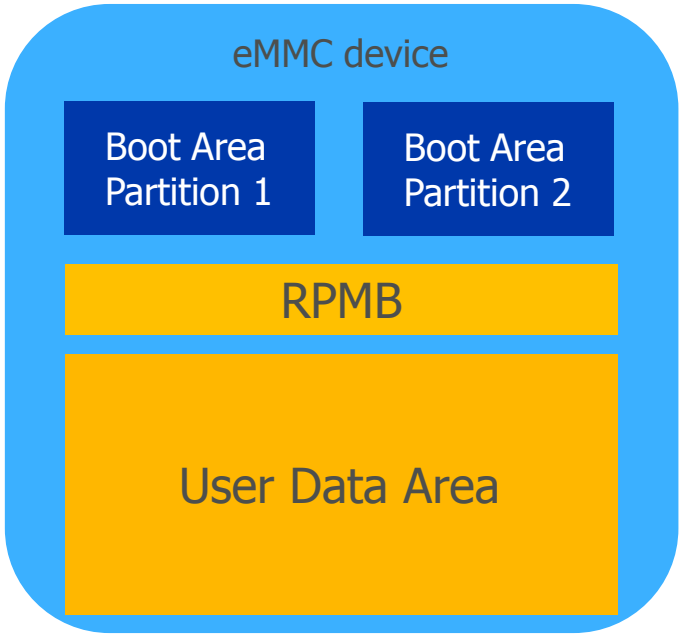
- Coverage: Boot, User, & General Area Partitions (no RPMB)
- Enable WP:
  - User: Set eCSD byte USER_WP bit US_PWR_WP_EN (eCSD[171:0])
  - Boot: Set eCSD byte BOOT_WP bit B_PWR_WP_EN (eCSD[173:0])
- Exceptions:
  - User/GPP: If eCSD byte USER_WP bit US_PWR_WP_DIS (eCSD[171:3]) is enabled, US_PWR_WP_EN eCSD[171:0] cannot be enabled
  - Boot: If eCSD byte BOOT_WP bit B_PWR_WP_DIS (eCSD[173:4]) is enabled, B_PWR_WP_EN eCSD[173:0] cannot be enabled
  - If temporary write protect is in enabled with TMP_WRITE_PROTECT, after a power cycle or hardware reset, the power-on protected area becomes temporary write protected

Card Lock/Unlock

Card Lock/Unlock is a password protection feature to protect the contents of the User Area using cmd42 from any access type (read/write/erase)

- Features include
  - Password: Password can be set, cleared, and reset with various lengths
  - Lock/Unlock: Locking the device separate can be done while simultaneously set the password; Unlocking cannot be done while clearing the password.
  - Erase: If password cannot be recalled, the entire User Area is forced erased and password cleared unless part of the user area has any area of permanent write protection
- Exception:
  - If PERM_PSWD_DIS (eCSD[171]) is enabled, no password protection features are possible
  - Boot, RPMB, and General partitions are not protected by lock/unlock features

Replay Protected Memory Block (RPMB)



Dedicated for data in an authenticated and replay-protected manner

First programming authentication key

The authentication key programming has to be managed in a secure environment like in an OEM production

Authentication key utilized to sign the read and write accesses made to the replay protected memory area with a Message Authentication (MAC)

The message authentication code (MAC) is calculated using HMAC SHA-256 as defined in [HMAC-SHA]

4.51/5.0 New Security Features

4.51 Sanitize

- The Sanitize operation remove physically data no longer required from the device.
- It improves the data security

5.0 SECURE_REMOVAL_TYPE

- Additional data security improvement through data erase
- Different processes of data removal can be selected by setting bits:
  - **0x0** : information removed by an erase of the physical memory
  - **0x1** : information removed by an overwriting the addressed locations with a character followed by an erase
  - **0x2** : information removed by an overwriting the addressed locations with a character, its complement, then a random character
  - **0x3** : information removed using a vendor defined


Micron®
Focused on Memory | Engineered for your Innovation