LEGAL NOTICE:

© Copyright 2008 to 2024 NVM Express®, Inc. ALL RIGHTS RESERVED.

This Technical Proposal is proprietary to the NVM Express, Inc. (also referred to as "Company") and/or its successors and assigns.

NOTICE TO USERS WHO ARE NVM EXPRESS, INC. MEMBERS: Members of NVM Express, Inc. have the right to use and implement this Technical Proposal subject, however, to the Member's continued compliance with the Company's Intellectual Property Policy and Bylaws and the Member's Participation Agreement.

NOTICE TO NON-MEMBERS OF NVM EXPRESS, INC.: If you are not a Member of NVM Express, Inc. and you have obtained a copy of this document, you only have a right to review this document or make reference to or cite this document. Any such references or citations to this document must acknowledge NVM Express, Inc. copyright ownership of this document. The proper copyright citation or reference is as follows: **"© 2008 to 2024 NVM Express, Inc. ALL RIGHTS RESERVED."** When making any such citations or references to this document you are not permitted to revise, alter, modify, make any derivatives of, or otherwise amend the referenced portion of this document in any way without the prior express written permission of NVM Express, Inc. Nothing contained in this document shall be deemed as granting you any kind of license to implement or use this document or the specification described therein, or any of its contents, either expressly or impliedly, or to any intellectual property owned or controlled by NVM Express, Inc., including, without limitation, any trademarks of NVM Express, Inc.

LEGAL DISCLAIMER:

THIS DOCUMENT AND THE INFORMATION CONTAINED HEREIN IS PROVIDED ON AN "**AS IS**" BASIS. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, NVM EXPRESS, INC. (ALONG WITH THE CONTRIBUTORS TO THIS DOCUMENT) HEREBY DISCLAIM ALL REPRESENTATIONS, WARRANTIES AND/OR COVENANTS, EITHER EXPRESS OR IMPLIED, STATUTORY OR AT COMMON LAW, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, VALIDITY, AND/OR NONINFRINGEMENT.

All product names, trademarks, registered trademarks, and/or servicemarks may be claimed as the property of their respective owners.

The NVM Express® design mark is a registered trademark of NVM Express, Inc.

NVM Express Workgroup
c/o VTM, Inc.
3855 SW 153rd Drive
Beaverton, OR 97003
USA
info@nvmexpress.org

Technical input submitted to the NVM Express® Workgroup is subject to the terms of the NVM Express® Participant's agreement. Copyright © 2008 to 2024 NVM Express, Inc.

NVM Express® Technical Proposal (TP)

Technical Proposal ID	**TP 4170 Boot Partition Write Protection**
Revision Date	**2024.03.27**
Builds on Specification(s)	**NVM Express Base Specification 2.0c** **NVM Express Management Interface Specification 1.2c**
References	**ECN 115** **TP 4074a Defining Scope for Features**

Technical Proposal Author(s)

Name	**Company**
Thomas Bowen	Intel
David Black	Dell
Mike Allison	Samsung
Andres Baez	Solidigm
Yoni Shternhell	Western Digital

Technical Proposal Overview

This proposal adds a new write protection control mechanism for Boot Partitions that is controllable through the Set Features command. Additionally, this proposal makes the RPMB based Boot Partition Protection mechanism optional.

Technical input submitted to the NVM Express® Workgroup is subject to the terms of the NVM Express® Participant's agreement. Copyright © 2008 to 2024 NVM Express, Inc.

Revision History

Revision Date	Change Description
2023.08.29	Initial draft
2023.08.31	Addressing Samsung feedback: • Incorporating ECN115 changes as the base this TP modifies • Added “controller” as scope for the new feature in this TP • Updated diagrams in section 8.2.3 to be more aligned to changes made in ECN115 • Defined default value for fields in new Feature • Clarified conflicting statement around resets to indicate that no other reset other than power cycle shall affect the write protection states in the new Feature Addressing Dell feedback: • Added statement in RPMB section blocking attempts to enable RPMB Boot Partition Write Protection when RPMB Boot Partition Write Protection is not supported. • Clarified Get and Set behaviors related to 000b (i.e., no change requested) for both fields in new Feature • Cleaned up handling of Set and Get for new Feature when RPMB Boot Partition Write Protection is enabled to allow clear indication that new Feature isn’t in use and RPMB Boot Partition Write Protection is enabled. Converted diagrams to visio diagrams
2023.09.06	Addressing Solidigm Feedback • Added missing references • Additional sentence added to handle the case when a Boot Partition is in a Write Unlocked state and a power cycle occurs • Added statement at top of section 8.2.3 that only one Boot Partition Write Protection mechanism is active at the same time Added subsections to section 8.2.3 to separate the three major parts of this section (Set Features Boot Partition Write Protection, RPMB Boot Partition Write Protection, and considerations when both mechanisms are supported)
2023.09.07	Added changes to NVM Express Management Interface to address support for new feature over NVM MI
2023.09.14	Addressing feedback from first review in NVMe TWG: • Added statement recommending only one boot partition write protection mechanism be supported by a controller to prevent malicious bypass of Write Protect Until Power Cycle. • Byte in Identify Controller data structure was renamed to “Boot Partition Capabilities” to allow for more general use of this byte. Existing “Boot Partition Write Protection Capabilities” field was limited to the three bits currently in use in the new “Boot Partition Capabilities” byte.
2023.10.03	Addressing additional feedback: • Cleaned up excess blank pages • Removed duplicate requirement around support of each capability from Identify Data structure section and cleaned up beginning of section 8.2.3 • Added statements to Boot Partition Write Protection fields in Boot Partition Write Protection Config Feature to indicate values that are not returned via Get Features (Change in state not requested) and not able to be set via Set Features (Write Protection controlled by RPMB)

Technical input submitted to the NVM Express® Workgroup is subject to the terms of the NVM Express® Participant’s agreement. Copyright © 2008 to 2024 NVM Express, Inc.

	• Added a sentence to section 8.2.3 indicating that boot partitions shared between controllers also share write protection states across controllers • Additional minor wording clean up in section 8.2.3 • Added a new requirement to section 8.18 preventing enablement of RPMB Boot Partition Write Protection when either boot partition is in a Write Locked Until Power Cycle state • Cleaned up diagrams in 8.2.3.1, 8.2.3.2, and 8.2.3.3 to have consistent state naming • Cleaned up 8.2.3.3 diagram to depict that you can only transition to an RPMB Boot Partition Write Protection Enabled state from a Write Locked or Write Unlocked state, but not a Write Locked Until Power Cycle state
2023.10.06	Updated text with new "Set Features Boot Partition Write Protection" naming to differentiate the following: • Boot Partition Write Protection: umbrella that consists of two capabilities: Set Features Boot Partition Write Protection and RPMB Boot Partition Write Protection • Set Features Boot Partition Write Protection (new in this revision): Capability that encompasses all write protection functionality that is controlled via the Boot Partition Write Protection Config Feature in Set Features • Boot Partition Write Protection Config: the feature in Set Features that is used to configure the Boot Partition Write Protection states that are a part of the Set Features Boot Partition Write Protection capability • RPMB Boot Partition Write Protection: write protection capability that was previously defined in NVMe 2.0 which controls Boot Partition Write Protection via RPMB Added new state definition tables to sections 8.2.3.1 and 8.2.3.2 to identify the states supported by each capability and whether each state is persistent across power cycles and controller level resets Revised new requirement/incompatible change statement Cleaned up definition of the value of 00b for the RPMB Boot Partition Write Protection Support field, moving most of the details to section 8.2.3 and added a reference to section 8.2.3 Added statement in section 8.18 to specify that the controller changes the values of the Boot Partition Write Protection State fields to a value of 100b in the Boot Partition Write Protection Config Feature when RPMB Boot Partition Write Protection is enabled Revised statement in section 5.27.1.TBD that prevented Set Features from changing the fields in the Boot Partition Write Protection Config Feature when RPMB Boot Partition Write Protection is enabled to instead prevent this when the fields are set to 100b (i.e., when Boot Partition Write Protection is controlled by RPMB) Revised Figure TBD1 (Boot Partition Write Protection Config Feature – Command Dword 11) to clarify that the value 000b is not returned via Get Features and 100b can not be set via Set Features
2023.10.26	Clarified statements related to both Boot Partition Write Protection capabilities being supported at the same time in section 8.2.3.3 Cleaned up capitalization of "Boot Partition" Clarified statement in section 8.18 preventing changes to either Boot Partition 0 Write Locked bit or Boot Partition 1 Write Locked bit when RPMB Boot Partition Write Protection is disabled Removed references to "PWRDIS". This topic will instead be covered in separate work from this TP to address considerations of power cycling a PCIe device
2023.11.01	Several editorial/cleanup changes made to sections 5.27.1.TBD, 8.2.2, and 8.2.3 based on feedback: • Copied restriction on when a value of 00b can be specified in the RPMB Boot Partition Write Protection Support field of Identify Controller into the value definition

Technical input submitted to the NVM Express® Workgroup is subject to the terms of the NVM Express® Participant's agreement. Copyright © 2008 to 2024 NVM Express, Inc.

	• Combined statements in section 5.27.1.TBD related to specifying a value of 000b for either Boot Partition • Standardized use of "field" when referring to either the Boot Partition 0 Write Protection State field or Boot Partition 1 Write Protection State field • Changed "set" to "cleared" when referring to value of 000b • Moved Get Features restriction related to value of 000b for either Boot Partition Write Protection State field • Fixed Notes cell width in Figure TBD1 Boot Partition Write Protection Config – Command Dword 11 • Changed most uses of "capability" to "mechanism" instead, leaving capability only used in the fields in the Identify Controller data structure • Other minor grammar cleanup Changed "should" to "shall" in statement in section 5.27.1.TBD to prohibit use of Write Locked Until Power Cycle state in multi-domain NVM subsystems Changed statement in section 8.2.3.1 to indicate Write Locked Until Power Cycle is prohibited in multi-domain NVM subsystems (aligning with "shall" described above. Added statement to section 8.2.3.3 to indicate supporting both Boot Partition write protection mechanisms is discouraged.
2023.11.02	Further cleanup of capitalization of "Boot Partition" Updated statement in section 8.2.3.1 prohibiting Write Locked Until Power Cycle in multi-domain NVM subsystems to make excessive reasoning text be listed as an example.
2023.11.29	First Phase 3 draft, containing the following changes: • Cleaned up capitalization of "feature" when referring to "this feature" or "Boot Partition Write Protection feature" • Fixed table spacing issues • Switched most instances of 'can' to 'may' or reworded to remove 'can' altogether • Cleaned up capitalization of "write protection" so that it is only capitalized when in a caption or formal name of a field or state • Renamed Figures TBD2, 413, and TBD5 to better align with naming convention used in existing Namespace Write Protect feature • Renamed section 8.2.3.3 to better align with NVMe section naming and capitalization convention
2023.12.07	Removed unmodified Notes portion of Figure 3 as it is not needed or modified in this TP Modified Notes in Figure TBD1 to avoid use of "can" or "may" Updated TP to accurately reflect references and modifications to ECN115 and TP4074 text with Orange and ~~Orange Strikethrough~~ text. Updated title of section 8.2.3.3 based on WG suggestion Cleaned up use of blue text in section 8.2.3.2 to properly identify text additions in section 8.2.3.2
2023.12.14	Added title for TP4074a to references section in header of document Added "field" in Note 2 of Figure TBD1 to better reflect the fields that are being referenced in the note
2024.01.23	Addressed 30-day Member Review comments: • Updated Copyright to 2024 • Capitalized "feature" in cases where "the Feature" or "this Feature" is used • Cleaned up grammar in section 5.27.1.TBD when referring to the Boot Partition 0 Write Protection State field and Boot Partition 1 Write Protection State field • Extended definition of "Feature Not Changeable" to more accurately reflect how it is being used for Namespace Write Protect and this TP

Technical input submitted to the NVM Express® Workgroup is subject to the terms of the NVM Express® Participant's agreement. Copyright © 2008 to 2024 NVM Express, Inc.

	• Cleaned up references to “host software” to instead more generically refer to “a host” or “the host” • Updated Figure 5 to reflect most recent changes in ECN115 • Removed wrapper “Boot Partition Write Protection Capabilities” field in Boot Partition Capabilities field of Identify Controller data structure • Cleaned up references in section 8.2.3 to new bits in Identify Data structure to only use “Boot Partition Capabilities” field rather than “Boot Partition Write Protection Capabilities” field • Grammar cleanup in section 8.2.2 to only use “Write Unlock” and “Write “Lock” as a state rather than a verb. • Reworded statement in section 8.2.3 related to host detection of support for RPMB Boot Partition Write Protection for controllers compliant to NVMe Base Specification 2.0 and earlier to avoid use of “if and only if” • Further cleanup of capitalization of “data structure”
2024.02.01	Deleted template instruction text from Description for Changes Document for NVM Express Base Specification 2.0c
2024.03.16	Integrated
2024.03.18	Added the controller support requirements for the new feature.
2024.03.27	Updated format of Figure TBD4 for clarity and editorial updates from Fred Knight and Thomas Bowen

Technical input submitted to the NVM Express® Workgroup is subject to the terms of the NVM Express® Participant’s agreement. Copyright © 2008 to 2024 NVM Express, Inc.

Description for Changes Document for NVM Express Base Specification 2.0c

New Features/Feature Enhancements/Required Changes:

- Add new Boot Partition write protection control mechanism to the Set Features command
  - Description of change
    - Add new Boot Partition write protection support fields in the Identify Controller data structure to identify support for the Set Features based Boot Partition Write Protection capability and the RPMB based Boot Partition Write Protection capability.
    - Add a new feature to the Set Features command that can be used to configure the write protection states of both Boot Partitions. This new feature can put either Boot Partition into one of the following states: Write Locked, Write Unlocked, or Write Locked Until Power Cycle.
  - New requirement / incompatible change
    - Previously RPMB Boot Partition Write Protection was required if Boot Partitions and RPMB were both supported. This version adds a new Boot Partition write protection capability and only requires one Boot Partition write protection capability be supported by a controller that supports Boot Partitions, making RPMB Boot Partition Write Protection optional so long as Set Features Boot Partition Write Protection is supported by the controller.
  - References
    - TP4170

Markup Conventions:

Black:	Unchanged (however, hot links are removed)
Orange:	Text from ECN115 or TP4074a
~~Orange Strikethrough:~~	Text added from ECN115 or TP4074a and deleted by this TP
~~Red Strikethrough~~:	Deleted
Blue:	New
Blue Highlighted:	TBD values, anchors, and links to be inserted in new text.
<Green Bracketed>:	Notes to editor

Technical input submitted to the NVM Express® Workgroup is subject to the terms of the NVM Express® Participant's agreement. Copyright © 2008 to 2024 NVM Express, Inc.

Description of Specification Changes for NVM Express Base Specification 2.0c

Modify a portion of section 3 as shown below:

…

3 NVM Express Architecture

3.1 NVM Controller Architecture

…

3.1.2 Controller Types

…

3.1.2.1 I/O Controller

…

3.1.2.1.3 Features Support

…

Figure 1: I/O Controller – Feature Support

Feature Name	Feature Support Requirements [1]	Logged in Persistent Event Log [1]
…		
Namespace Write Protection Config	O	O
Boot Partition Write Protection Config	O	O
…		
Notes: 1. O/M/P/NR definition: O = Optional, M = Mandatory, P = Prohibited, NR = Not Recommended 2. …		

Technical input submitted to the NVM Express® Workgroup is subject to the terms of the NVM Express® Participant's agreement. Copyright © 2008 to 2024 NVM Express, Inc.

…

3.1.2.2 Administrative Controller

…

3.1.2.2.3 Features Support

…

Figure 2: Administrative Controller – Feature Support

Feature Name	Feature Support Requirements [1]	Logged in Persistent Event Log [1]
…		
Namespace Write Protection Config	O	O
Boot Partition Write Protection Config	O	O
…		
Notes: 1. O/M/P/NR definition: O = Optional, M = Mandatory, P = Prohibited, NR = Not Recommended. 2. …		

…

3.1.2.3 Discovery Controller

…

3.1.2.4 Features Support

…

Figure 3: Discovery Controller – Feature Support

Feature Name	Feature Support Requirements [1]	Logged in Persistent Event Log [1]
…		
Namespace Write Protection Config	P	P
Boot Partition Write Protection Config	P	P
…		
Notes: 1. O/M/P/NR definition: O = Optional, M = Mandatory, P = Prohibited, NR = Not Recommended. 2. …		

Technical input submitted to the NVM Express® Workgroup is subject to the terms of the NVM Express® Participant's agreement. Copyright © 2008 to 2024 NVM Express, Inc.

…

Modify a portion of section 5 as shown below:

…

5 Admin Command Set

…

5.12 Firmware Commit command

…

When modifying Boot Partitions, the host may select the Boot Partition to mark as active or to replace. A Boot Partition is only able to be written when write unlocked (refer to section 8.2).

…

5.12.1 Command Completion

…

Figure 183: Firmware Commit – Command Specific Status Values

Value	Description
…	
1Eh	**Boot Partition Write Prohibited:** This error is indicated if a command attempts to modify a Boot Partition while write locked (refer to section 8.2.3).
…	

…

5.15 Get Features command

…

Figure 194: Get Features – Feature Identifiers

Description	Section Defining Format of Attributes Returned
…	
Namespace Write Protection Config	5.27.1.28
…	
Spinup Control	5.27.1.22
Boot Partition Write Protection Config	5.27.1.TBD
I/O Command Set specific features	I/O Command Set specification

…

5.17 Identify command

…

Technical input submitted to the NVM Express® Workgroup is subject to the terms of the NVM Express® Participant's agreement. Copyright © 2008 to 2024 NVM Express, Inc.

5.17.2 Identify Data Structures

…

5.17.2.1 Identify Controller Data Structure (CNS 01h)

…

Figure 275: Identify - Identify Controller Data Structure, I/O Command Set Independent

<table>
<tr><th>Bytes</th><th>I/O[1]</th><th>Admin[1]</th><th>Disc[1]</th><th>Description</th></tr>
<tr><td colspan="5">…</td></tr>
<tr><td>102</td><td>M</td><td>R</td><td>R</td><td>Boot Partition Capabilities (BPCAP): This field indicates the Boot Partition capabilities supported by the controller.
<table>
<tr><th>Bits</th><th>Description</th></tr>
<tr><td>07:03</td><td>Reserved</td></tr>
<tr><td>02</td><td>Set Features Boot Partition Write Protection Support (SFBPWPS): This bit indicates if Set Features Boot Partition Write Protection is supported by the controller. When supported, this capability allows a host to configure Boot Partition write protection states via the Boot Partition Write Protection Config feature in the Set Features command. Refer to section 8.2.3.1.
<table>
<tr><th>Value</th><th>Definition</th></tr>
<tr><td>0b</td><td>Set Features Boot Partition Write Protection is not supported by this controller.</td></tr>
<tr><td>1b</td><td>Set Features Boot Partition Write Protection is supported by this controller.</td></tr>
</table></td></tr>
<tr><td>01:00</td><td>RPMB Boot Partition Write Protection Support (RPMBBPWPS): This field indicates if RPMB Boot Partition Write Protection is supported by the controller. When supported, this capability allows a host to configure Boot Partition write protection states via RPMB. Refer to section 8.2.3.2.
<table>
<tr><th>Value</th><th>Definition</th></tr>
<tr><td>00b</td><td>Support for RPMB Boot Partition Write Protection is not specified. Only controllers compliant with NVM Express Base Specification, Revision 2.0 and earlier are allowed to report this value. Refer to section 8.2.3 for more details on when a controller may return this value.</td></tr>
<tr><td>01b</td><td>RPMB Boot Partition Write Protection is not supported by this controller.</td></tr>
<tr><td>10b</td><td>RPMB Boot Partition Write Protection is supported by this controller.</td></tr>
<tr><td>11b</td><td>Reserved</td></tr>
</table></td></tr>
</table></td></tr>
<tr><td>110:
103~~102~~</td><td></td><td></td><td></td><td>Reserved</td></tr>
<tr><td colspan="5">…</td></tr>
</table>

…

5.27 Set Features command

…

Technical input submitted to the NVM Express® Workgroup is subject to the terms of the NVM Express® Participant's agreement. Copyright © 2008 to 2024 NVM Express, Inc.

5.27.1 Feature Specific Information

…

Figure 316: Set Features – Feature Identifiers

Feature Identifier	Current Setting Persists Across Power Cycle and Reset [2]	Uses Memory Buffer for Attributes	Feature Name	Scope
…				
83h	Yes	No	Reservation Persistence	Namespace
84h	No	No	Namespace Write Protection Config	Namespace
85h	No	No	Boot Partition Write Protection Config	Controller
86h~~85h~~ to BFh			Reserved	
C0h to FFh			Vendor Specific[1, 5]	
…				

…

5.27.1.TBD Boot Partition Write Protection Config (Feature Identifier 85h)

This Feature is used by the host to configure Boot Partition write protection states and to determine the write protection state of both Boot Partitions supported by a controller. Refer to section 8.2.3.1 for definition and behaviors of the Boot Partition write protection states and state transitions. The settings are specified in Command Dword 11.

This Feature is not saveable (refer to Figure 195). The default value of both the Boot Partition 0 Write Protection State field and the Boot Partition 1 Write Protection State field after a power cycle is Write Locked.

If a Get Features command is submitted for this Feature, the attributes specified in Figure TBD1 are returned in Dword 0 of the completion queue entry for that command. A controller shall not return a value of 000b for either the Boot Partition 0 Write Protection State field or the Boot Partition 1 Write Protection State field as a result of the Get Features command for the Boot Partition Write Protection Config feature.

If a Set Features command is submitted for this Feature with either the Boot Partition 0 Write Protection State field or the Boot Partition 1 Write Protection State field cleared to 000b, then the controller shall not change the Boot Partition write protection state for that Boot Partition as part of the Set Features command completion.

If the Boot Partition Write Protection Enable bit is set to '1' in the RPMB Device Configuration Block data structure (refer to section 8.18), then the controller shall return a value of 100b for both the Boot Partition 0 Write Protection State field and the Boot Partition 1 Write Protection State field as a result of the Get Features command for the Boot Partition Write Protection Config feature.

If a Set Features command is submitted for this Feature with either the Boot Partition 0 Write Protection State field or the Boot Partition 1 Write Protection State field set to 100b, then the controller shall abort the command with a status code of Invalid Field in Command.

Technical input submitted to the NVM Express® Workgroup is subject to the terms of the NVM Express® Participant's agreement. Copyright © 2008 to 2024 NVM Express, Inc.

Figure TBD1 Boot Partition Write Protection Config - Command Dword 11

<table>
<tr><th>Bits</th><th>Description</th></tr>
<tr><td>31:06</td><td>Reserved</td></tr>
<tr><td>05:03</td><td>Boot Partition 1 Write Protection State (BP1WPS): This field specifies the write protection state of Boot Partition 1.

The default value of this field is Write Locked.

<table>
<tr><th>Value</th><th>Definition</th></tr>
<tr><td>000b[1]</td><td>Change in state not requested</td></tr>
<tr><td>001b</td><td>Write Unlocked</td></tr>
<tr><td>010b</td><td>Write Locked</td></tr>
<tr><td>011b</td><td>Write Locked Until Power Cycle</td></tr>
<tr><td>100b[2]</td><td>Write Protection controlled by RPMB</td></tr>
<tr><td>101b to 111b</td><td>Reserved</td></tr>
</table></td></tr>
<tr><td>02:00</td><td>Boot Partition 0 Write Protection State (BP0WPS): This field specifies the write protection state of Boot Partition 0.

The default value of this field is Write Locked.

<table>
<tr><th>Value</th><th>Definition</th></tr>
<tr><td>000b[1]</td><td>Change in state not requested</td></tr>
<tr><td>001b</td><td>Write Unlocked</td></tr>
<tr><td>010b</td><td>Write Locked</td></tr>
<tr><td>011b</td><td>Write Locked Until Power Cycle</td></tr>
<tr><td>100b[2]</td><td>Write Protection controlled by RPMB</td></tr>
<tr><td>101b to 111b</td><td>Reserved</td></tr>
</table></td></tr>
<tr><td colspan="2">Notes:
1. A value of 000b is not returned by a controller via a Get Features command. This value is only used in the Set Features command.
2. A value of 100b is reserved for the Set Features command for both the Boot Partition 0 Write Protection State field and the Boot Partition 1 Write Protection State field. The Boot Partition write protection states transition to this state when RPMB Boot Partition Write Protection is enabled (refer to section 8.2.3.2 and section 8.18).</td></tr>
</table>

If a Set Features command is submitted that attempts to change the Boot Partition write protection state of a Boot Partition that is in the Write Locked Until Power Cycle state, then the controller shall abort the command with a status code of Feature Not Changeable.

If a Set Features command is submitted that attempts to change either Boot Partition write protection state from a value of 100b (i.e., Boot Partition write protection is controlled by RPMB), then the controller shall abort the command with a status code of Feature Not Changeable.

If a Set Features command attempts to change the Boot Partition write protection state of a Boot Partition shared across multiple controllers to the Write Locked Until Power cycle state in a multi-domain NVM subsystem (i.e., the MDS bit is set to '1' in the CTRATT field of the Identify Controller data structure (refer to Figure 275), then the controller shall abort the command with a status code of Feature Not Changeable.

5.27.2 Command Completion

…

Figure 370: Set Features – Command Specific Status Values

Value	Description
…	

Technical input submitted to the NVM Express® Workgroup is subject to the terms of the NVM Express® Participant's agreement. Copyright © 2008 to 2024 NVM Express, Inc.

Figure 370: Set Features – Command Specific Status Values

Value	Description
0Eh	**Feature Not Changeable:** The Feature Identifier specified does not support a changeable value or the value is not changeable at this time.
…	

Modify a portion of section 8 as shown below:

…

8 Extended Capabilities

…

8.2 Boot Partitions

Boot Partitions provide an optional area of NVM storage that may be read by the host without the host initializing queues or enabling the controller. The simplified interface to access Boot Partitions may be used for platform initialization code (e.g., a bootloader that is executed from host ROM) to boot to a pre-OS environment (e.g., UEFI) instead of storing the image on another non-volatile storage medium (e.g., SPI flash). Refer to section 8.2.1 for the procedure to read the contents of a Boot Partition.

A controller that supports Boot Partitions has two Boot Partitions of equal size using Boot Partition identifiers 0h and 1h. The two Boot Partitions allow the host to update one and verify the contents before marking the Boot Partition active. Controllers in the NVM subsystem may share the same Boot Partitions.

The contents of Boot Partitions are only modified using the Firmware Image Download and Firmware Commit commands (refer to section 8.2.2) and may be secured using either the Boot Partition Write Protection Config feature or the Replay Protected Memory Block to prevent unauthorized modifications (refer to section 8.2.3).

…

8.2.2 Writing to a Boot Partition

…

The process for updating a Boot Partition is:

1. The host issues a Firmware Image Download command to download the contents of the Boot Partition to a controller. There may be multiple portions of the Boot Partition to download, thus the offset for each portion of the Boot Partition being downloaded is specified in the Firmware Image Download command. A ~~H~~host ~~software~~ shall send the Boot Partition image in order starting with the beginning of the Boot Partition;
2. The host transitions the ~~Unlock~~ Boot Partition~~s~~ that is to be updated to the Write Unlocked State~~for writing~~ (refer to section 8.2.3);
3. The host submits a Firmware Commit command (refer to section 5.12) on that controller with a Commit Action of 110b which specifies that the downloaded image replaces the contents of the Boot Partition specified in the Boot Partition ID field;
4. The controller completes the Firmware Commit command. The following actions are taken in certain error scenarios:

Technical input submitted to the NVM Express® Workgroup is subject to the terms of the NVM Express® Participant's agreement. Copyright © 2008 to 2024 NVM Express, Inc.

a. If the firmware activation was not successful because the Boot Partition could not be written, then the controller reports an error of Boot Partition Write Prohibited;

5. (Optional) The host reads the contents of the Boot Partition to verify they are correct (refer to section 8.2.1). A h~~H~~ost ~~software~~ updates the active Boot Partition ID by issuing a Firmware Commit command with a Commit Action of 111b; and
6. The host transitions ~~locks~~ the Boot Partition to either the Write Locked State or Write Locked Until Power Cycle State~~access~~ to prevent further modification (refer to section 8.2.3).

…

8.2.3 Boot Partition Write Protection

~~A controller that supports Boot Partitions and RPMB shall support Boot Partition Protection.~~ A controller that supports both Boot Partitions and RPMB shall support at least one of the following Boot Partition write protection mechanisms:

- Set Features Boot Partition Write Protection (refer to section 8.2.3.1); or
- RPMB Boot Partition Write Protection (refer to section 8.2.3.2).

It is not recommended that a controller support both Set Features Boot Partition Write Protection and RPMB Boot Partition Write Protection.

A controller that supports Boot Partitions and does not support RPMB shall support Set Features Boot Partition Write Protection.

A host is able to determine whether Set Features Boot Partition Write Protection is supported by checking the value of the Set Features Boot Partition Write Protection Support bit of the Boot Partition Capabilities field in the Identify Controller Data Structure (refer to Figure 275).

A host is able to determine whether RPMB Boot Partition Write Protection is supported by checking the RPMB Boot Partition Write Protection Support field of the Boot Partition Capabilities field in the Identify Controller data structure (refer to Figure 275). Only controllers compliant with NVM Express Base Specification, Revision 2.0 and earlier are allowed to report a value of 00b (i.e., support not specified) in that field. If a controller reports the 00b value, a host is able to determine if RPMB Boot Partition Write Protection is supported by checking whether the controller supports both Boot Partitions (refer to section 3.1.3.1) and RPMB (refer to section 5.17.2.1) because a controller compliant with NVM Express Base Specification, Revision 2.0 and earlier is required to support RPMB Boot Partition Write Protection when the controller supports both Boot Partitions and RPMB.

If Set Features Boot Partition Write Protection is supported and either:

1) RPMB Boot Partition Write Protection is not supported; or
2) RPMB Boot Partition Write Protection is not enabled,

then the Boot Partition write protection states are able to be configured via the Boot Partition Write Protection Config feature. Section 8.2.3.1 covers the case when only the Boot Partition Write Protection Config feature is supported.

If RPMB Boot Partition Write Protection is supported and enabled, then the Boot Partition write ~~P~~protection states are able to ~~may~~ be configured using RPMB (refer to section 8.18). Section 8.2.3.2 covers the case where only RPMB Boot Partition Write Protection is supported.

Only one mechanism controls the Boot Partition write protection states at a time. Section 8.2.3.3 covers considerations when both Boot Partition write protection mechanisms are supported.

If any Boot Partition is shared across multiple controllers (refer to section 8.2), then the write protection state of the Boot Partition shall be enforced by all controllers that share that Boot Partition.

8.2.3.1 Set Features Boot Partition Write Protection

Figure TBD2 shows an overview of the Boot Partition write protection states for each Boot Partition when only Set Features Boot Partition Write Protection is supported.

Technical input submitted to the NVM Express® Workgroup is subject to the terms of the NVM Express® Participant's agreement. Copyright © 2008 to 2024 NVM Express, Inc.

Figure TBD2: Set Features Boot Partition Write Protection State Machine Model

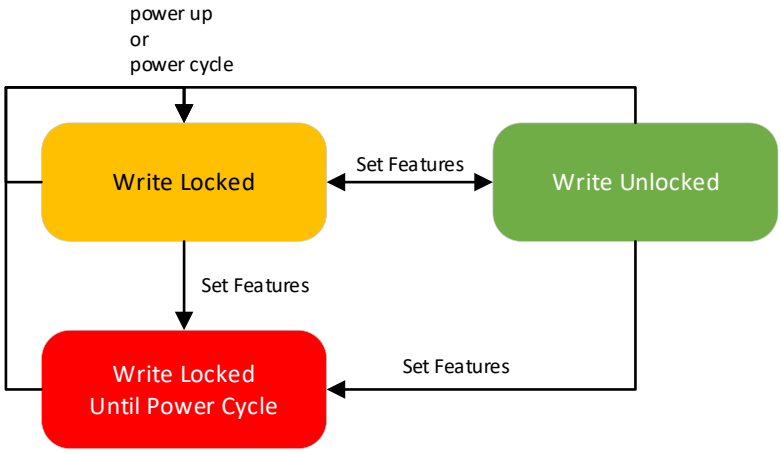


Figure TBD3 defines the write protection states per Boot Partition if Set Features Boot Partition Write Protection is supported.

Figure TBD3: Set Features Boot Partition Write Protection State Definitions

State	Definition	Persistent Across	
		Power Cycles	Controller Level Resets
Write Unlocked	The Boot Partition is not write locked.	No	Yes
Write Locked	The Boot Partition is write locked.	Yes	Yes
Write Locked Until Power Cycle	The Boot Partition is write locked until the next power cycle.	No	Yes

If Set Features Boot Partition Write Protection is supported, then the default state for all Boot Partitions is the Write Locked state. In this state, a host may read from a Boot Partition but is unable to modify that Boot Partition. To enable modification of a Boot Partition, a host has to first transition the Boot Partition to the Write Unlocked state by setting the appropriate Boot Partition Write Protection State to Write Unlocked using the Boot Partition Write Protection Config feature via the Set Features command.

In the Write Unlocked state, a host may read from and modify a Boot Partition. Any Boot Partition in a Write Unlocked state returns back to the Write Locked state when the controller undergoes a power cycle.

If Set Features Boot Partition Write Protection is supported, then both Boot Partitions support a Write Locked Until Power Cycle state. In this state, the Boot Partition can be read from but is prohibited from being modified. Additionally, once a Boot Partition enters the Write Locked Until Power Cycle state, the Boot Partition remains in this state until the controller is power cycled.

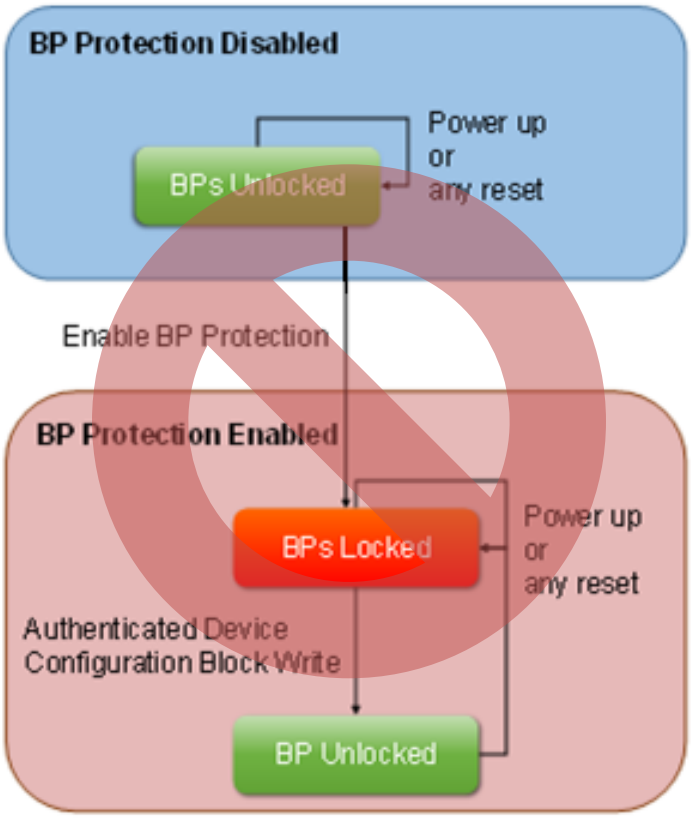
Technical input submitted to the NVM Express® Workgroup is subject to the terms of the NVM Express® Participant's agreement. Copyright © 2008 to 2024 NVM Express, Inc.

The Write Locked Until Power Cycle state is prohibited in multi-domain NVM subsystems with Boot Partitions shared across controllers (e.g., since clearing that state requires simultaneous power cycle of all controllers that share the Boot Partitions). The result of a command that attempts to use that state in a multi-domain NVM subsystem is specified in section 5.27.1.TBD.

8.2.3.2 RPMB Boot Partition Write Protection

Figure 413 shows an overview of the Boot Partition write ~~P~~protection states for each Boot Partition when only RPMB Boot Partition Write Protection is supported.

Figure 413: RPMB Boot Partition Write Protection State Machine Model~~Overview~~



<Note to editor: Replace Figure 413 with diagram below>

Technical input submitted to the NVM Express® Workgroup is subject to the terms of the NVM Express® Participant's agreement. Copyright © 2008 to 2024 NVM Express, Inc.

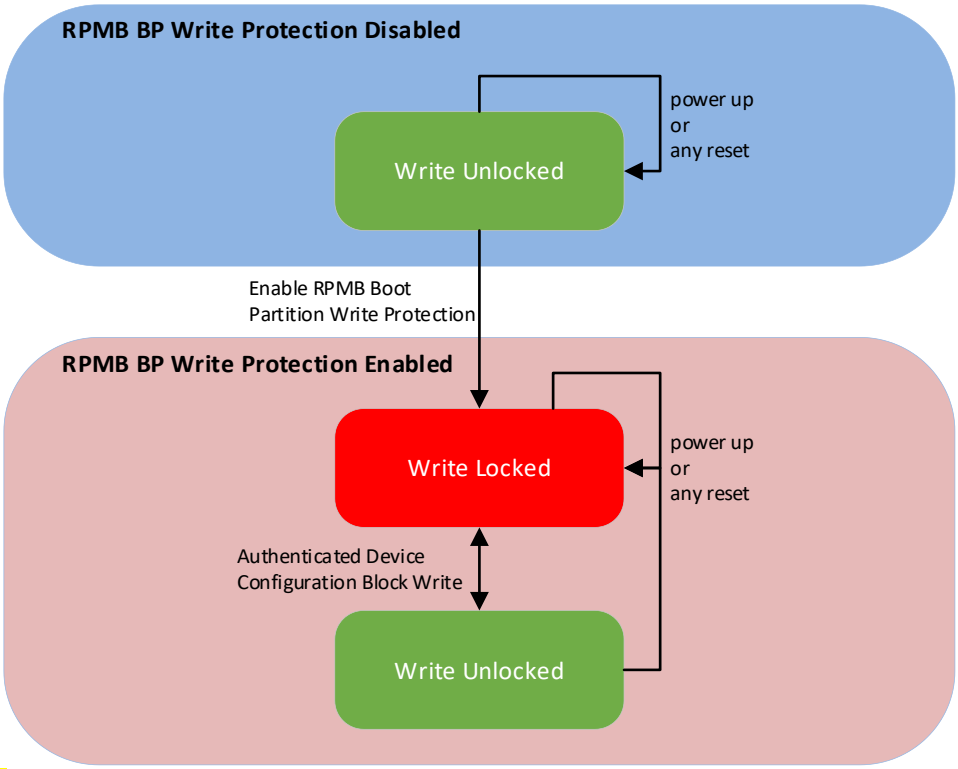


Figure TBD4 defines the write protection states per Boot Partition if RPMB Boot Partition Write Protection is supported.

Figure TBD4: RPMB Boot Partition Write Protection State Definitions

State	Definition	Persistent Across	
		Power Cycles	Controller Level Resets
RPMB Boot Partition Write Protection Disabled			
Write Unlocked	The Boot Partition is not write locked.	Yes	Yes
RPMB Boot Partition Write Protection Enabled			
Write Unlocked	The Boot Partition is not write locked.	No	No
Write Locked	The Boot Partition is write locked.	Yes	Yes

If Set Features Boot Partition Write Protection is not supported by the controller, then p~~P~~rior to ~~activating~~enabling RPMB Boot Partition Write Protection, the default state for all Boot Partitions is the "Write Unlocked~~"~~ state. ~~In this state, host software may read and write a Boot Partition.~~If Set Features Boot Partition Write Protection is also supported by the controller, then the default state for all Boot Partitions is the Write Locked state, regardless of whether RPMB Boot Partition Write Protection has been enabled or not. Refer to section 8.2.3.1 for more details on Boot Partition write protection when RPMB Boot Partition Write Protection is disabled and section 8.2.3.3 for additional considerations when both Boot Partition write protection capabilities are supported.

If Set Features Boot Partition Write Protection is not supported by the controller, then ~~A~~all Boot Partitions remain unlocked until RPMB Boot Partition Write Protection is enabled by the host ~~software~~. A h~~H~~ost ~~software~~ enables RPMB Boot Partition Write Protection by setting the Boot Partition Write Protection Enabled bit in the RPMB Device Configuration Block data structure (refer to section 8.18). Once RPMB Boot Partition Write Protection is enabled, the controller shall reject Authenticated Device Configuration Block Writes that attempt to disable the RPMB Boot Partition Write Protection mechanism (i.e., enabling RPMB Boot Partition Write Protection is permanent). Once RPMB Boot Partition Write Protection is enabled, Boot Partitions are able to be modified only after write unlocking the Boot Partition using RPMB.

Technical input submitted to the NVM Express® Workgroup is subject to the terms of the NVM Express® Participant's agreement. Copyright © 2008 to 2024 NVM Express, Inc.

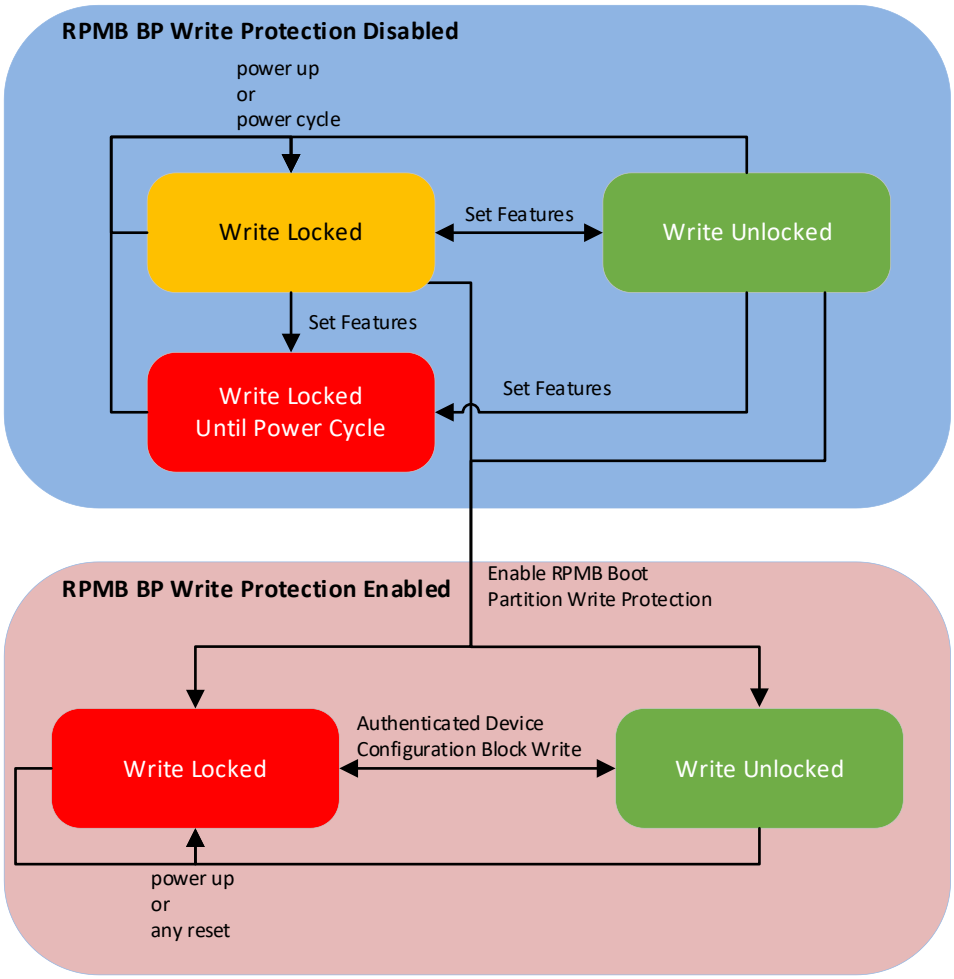
After ~~activating~~enabling RPMB Boot Partition Write Protection:

a) The default state for all Boot Partitions is the ~~"~~Write Locked~~"~~ state. In this state, a host ~~software~~ may read a Boot Partition. In this state, the controller rejects attempts to write to a Boot Partition using the Firmware Commit command.
b) Each Boot Partition may be locked or unlocked independently using the corresponding bit in the Device Configuration Block data structure. A Boot Partition may be unlocked in the same command that enables RPMB Boot Partition Write Protection; and
c) If any Boot Partition has been unlocked, a power cycle or Controller Level Reset event results in that Boot Partition becoming write locked.

8.2.3.3 Interactions between Boot Partition Write Protection Mechanisms

Figure TBD5 shows an overview of the Boot Partition write protection states for each Boot Partition when both Boot Partition write protection mechanisms are supported. Supporting both Boot Partition write protection mechanisms is discouraged, as specified in section 8.2.3.

Figure TBD5: Boot Partition Write Protection State Machine Model



If both Boot Partition write protection mechanisms are supported by the controller, only one Boot Partition write protection mechanism controls the write protection states of the Boot Partitions for the controller at any time. If RPMB Boot Partition Write Protection is enabled, then RPMB Boot Partition Write Protection controls the Boot Partition write protection states (refer to section 8.2.3.2 and section 8.18). If RPMB Boot

Technical input submitted to the NVM Express® Workgroup is subject to the terms of the NVM Express® Participant's agreement. Copyright © 2008 to 2024 NVM Express, Inc.

Partition Write Protection is disabled, then Set Features Boot Partition Write Protection controls the Boot Partition write protection states (refer to section 8.2.3.1 and section 5.27.1.TBD). Control of the Boot Partition write protection states transitions from Set Features Boot Partition Write Protection to RPMB Boot Partition Write Protection by enabling RPMB Boot Partition Write Protection when the Boot Partitions are in either a Write Unlocked or Write Locked state.

If both Boot Partition write protection capabilities are supported and an RPMB authentication key has not been programmed for RPMB target 0, there is a possibility of malicious bypass of a Boot Partition's Write Locked Until Power Cycle state. In order to prevent malicious bypass of a Boot Partition's Write Locked Until Power Cycle state, a controller that supports both Boot Partition write protection mechanisms is required to prevent host attempts to enable RPMB Boot Partition Write Protection when either Boot Partition is in a Write Locked Until Power Cycle state. Refer to section 8.18 for the specific behavior that the controller exhibits under this condition.

…

8.18 Replay Protected Memory Block

The Replay Protected Memory Block (RPMB) provides a means for the system to store data to a specific memory area in an authenticated and replay protected manner. This is provided by first programming authentication key information to the controller that is used as a shared secret. The system is not authenticated in this phase, therefore the authentication key programming should be done in a secure environment (e.g., as part of the manufacturing process). The authentication key is utilized to sign the read and write accesses made to the replay protected memory area with a Message Authentication Code (MAC). Use of random number (nonce) generation and a write count property provide additional protection against replay of messages where messages could be recorded and played back later by an attacker.

Any access attempts to the replay protected memory area prior to the Authentication Key being programmed results in an RPMB Operation Result Operation Status of 07h (i.e., Authentication Key not yet programmed) (refer to Figure 462). Once the key is programmed, this Result value shall no longer be used.

An Authenticated Data Write to the RPMB Device Configuration Block data structure that attempts to set the Boot Partition Write Protection Enabled bit when RPMB Boot Partition Write Protection is not supported results in an RPMB Operation Result Operation Status of 05h (i.e., Write failure in the RPMB Operation Status field) (refer to Figure 462).

An Authenticated Data Write to the RPMB Device Configuration Block data structure that attempts to set the Boot Partition Write Protection Enabled bit when either Boot Partition is in the Write Locked Until Power Cycle state (refer to section 5.27.1.TBD and section 8.2.3.1) results in an RPMB Operation Result Operation Status of 05h (i.e., Write failure in the RPMB Operation Status field) (refer to Figure 462).

An Authenticated Data Write to the RPMB Device Configuration Block data structure that attempts to ~~set the~~ change either the Boot Partition 0 Write Locked bit or the Boot Partition 1 Write Locked bit when the Boot Partition Write Protection Enabled bit is ~~disabled~~ cleared to '0' results in an RPMB Operation Result Operation Status of 05h (i.e., Write failure in the RPMB Operation Status field) (refer to Figure 462).

If Set Features Boot Partition Write Protection is supported, then an Authenticated Data Write to the RPMB Device Configuration Block data structure that successfully enables RPMB Boot Partition Write Protection shall also result in the controller changing the Boot Partition 0 Write Protection State and Boot Partition 1 Write Protection State values in the Boot Partition Write Protection Config feature to a value of 100b to indicate that Boot Partition write protection is controlled by RPMB.

The controller may support multiple RPMB targets. RPMB targets are not contained within a namespace. Controllers in the NVM subsystem may share the same RPMB targets. Security Send and Security Receive commands for RPMB do not use the namespace ID field; NSID shall be cleared to 0h. Each RPMB target operates independently – there may be requests outstanding to multiple RPMB targets at once (where the requests may be interleaved between RPMB targets). In order to guarantee ordering the host should issue

Technical input submitted to the NVM Express® Workgroup is subject to the terms of the NVM Express® Participant's agreement. Copyright © 2008 to 2024 NVM Express, Inc.

and wait for completion for one Security Send or Security Receive command at a time. Each RPMB target requires individual authentication and key programming. Each RPMB target may have its own unique Authentication Key.

The message types defined in Figure 461 are used by the host to communicate with an RPMB target. Request Message Types are sent from the host to the controller. Response Message Types are sent to the host from the controller.

Figure 460 defines the RPMB Device Configuration Block data structure – the non-volatile contents stored within the controller for RPMB target 0.

Figure 460: RPMB Device Configuration Block Data Structure

<table>
<tr><th>Bytes</th><th>Type</th><th>Component Name</th><th>Description</th></tr>
<tr><td>00</td><td>RW</td><td>Boot Partition Protection Enable</td><td>Boot Partition Protection Enable: This field specifies whether Boot Partition Protection is enabled.
<table>
<tr><th>Bits</th><th>Description</th></tr>
<tr><td>7:1</td><td>Reserved</td></tr>
<tr><td>0</td><td>Boot Partition Write Protection Enabled: If this bit is set to ‘1’, then RPMB Boot Partition Write Protection is enabled.
If this bit is cleared to ‘0’, then RPMB Boot Partition Write Protection is disabled or not supported. Once enabled, the controller shall prevent disabling RPMB Boot Partition Write Protection.</td></tr>
</table></td></tr>
<tr><td>01</td><td>RW</td><td>Boot Partition ~~Lock~~ Protection State</td><td>Boot Partition ~~Lock Status~~Protection State: This field specifies the current ~~status of the~~ Boot Partition protection state when RPMB Boot Partition Write Protection is enabled~~Lock~~. This field shall be cleared to 0h unless RPMB Boot Partition Write Protection is enabled. Refer to section 8.2.3.
<table>
<tr><th>Bits</th><th>Description</th></tr>
<tr><td>7:2</td><td>Reserved</td></tr>
<tr><td>1</td><td>Boot Partition ~~Protection~~ 1 Write Locked: If this bit is set to ‘1’, then ~~the~~ Boot Partition 1 (i.e., the BPID bit in Figure 181 is set to ‘1’) is write locked.
If this bit is cleared to ‘0’, then ~~the~~ Boot Partition 1 is write unlocked.</td></tr>
<tr><td>0</td><td>Boot Partition ~~Protection~~ 0 Write Locked: If this bit is set to ‘1’, then ~~the~~ Boot Partition 0 (i.e., the BPID bit in Figure 181 is cleared to ‘0’) is write locked.
If this bit is cleared to ‘0’, then ~~the~~ Boot Partition 0 (i.e., BPID is 0) is write unlocked.</td></tr>
</table></td></tr>
<tr><td>…</td><td>…</td><td>…</td><td>…</td></tr>
</table>

Description of Specification Changes for NVM Express Management Interface Specification 1.2c

Modify section 6 as shown below:

6 NVM Express Admin Command Set

…

6.5 Set Features and Get Features

…

Technical input submitted to the NVM Express® Workgroup is subject to the terms of the NVM Express® Participant’s agreement. Copyright © 2008 to 2024 NVM Express, Inc.

Figure 127: Management Endpoint - Feature Support

Feature Name[2]	Feature Identifier	Support Requirements[1]	
		NVMe Storage Device	NVMe Enclosure
…			
Namespace Write Protection Config	84h	P	P
Boot Partition Write Protection Config	85h	P	P
Vendor Specific	C0h to FFh	O	O
Notes: 1. O = Optional, M = Mandatory, P = Prohibited for Set Features/Optional for Get Features. 2. Refer to the NVM Express Base Specification unless another footnote specifies otherwise. 3. Refer to the NVM Command Set Specification. 4. Refer to the Key Value Command Set Specification.			

…

Technical input submitted to the NVM Express® Workgroup is subject to the terms of the NVM Express® Participant's agreement. Copyright © 2008 to 2024 NVM Express, Inc.