LEGAL NOTICE:

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: **“© 2007 to 2023 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

NVM Express Technical Proposal for New Feature

Technical Proposal ID	**TP 8013a**
Change Date	**2021-07-06**
Builds on Specification	**NVM Express Base 2.0**
Technical Proposal that build on this technical proposal	**TP8017 Discovery Subsystem Authentication Recommendations**

Technical Proposal Author(s)

Name	**Company**
Curtis Ballard, Matt Goepfert	HPE
Fred Knight	NetApp

Currently, only the well-known Discovery Service NQN (nqn.2014-08.org.nvmexpress.discovery) exists to identify a Discovery subsystem, which is used by all Discovery subsystems. With the advent of TP 8006 (NVMe-oF In Band Authentication), there should be a unique NQN provided as a parameter when performing NVMe in-band authentication using DH-HMAC-CHAP. This technical proposal defines a unique NQN which Discovery subsystems can supply when performing NVMe in-band authentication using DH-HMAC-CHAP, or for other purposes (e.g., for hosts to detect if Discovery controllers are contained in different Discovery subsystems or not).

Refer to TP8017 Discovery Subsystem Authentication Recommendations as that technical proposal updated all instances of “unique NQN” in this technical proposal to “unique Discovery Service NQN” to make it more consistent with the term “well-known Discovery Service NQN”.

Revision History

Revision Date	**Change Description**
2021-04-15	Initial version
2021-04-19	• Changed “Discovery Service” to “Discovery subsystem” globally throughout the doc (except for “well-known Discovery Service NQN”) • Made changes to section 3.1.2.3 based upon feedback from Curtis and Fred
2021-04-21	• Made changes to section 3.1.2.3 based up 4/20 FMDS feedback • Added text to section 8.13.2 that in-band authentication shouldn’t be performed using the well-known Discovery Service NQN if a Discovery subsystem provides a unique NQN
2021-04-28	• Further restructuring changes to section 3.1.2.3 based upon FMDS feedback • Added additional text to section 8.13.2 about host detecting existence of unique NQN as it relates to in-band authentication
2021-05-05	• Accepted all changes and deleted all closed comments • Added Fred Knight as an author
2021-05-18	• Changed document name to indicate that it is in phase 3
2021-07-01	• Changed document name to indicate that it is entering integration
2021-07-06	• Integrated into the NVMe Base Specification, revision 2.0.

2023-01-19	• Added statement referring to TP8017 for changes affecting this technical proposal and updated markup conventions.

Markup conventions

Style	Meaning
Black	Unchanged existing material
Blue	New material added by TP8013
Orange	New material added by TP8013a
~~Red~~	Existing material to be deleted
Blue	New material to be renumbered as incorporated
<Green>	Note to the editor

Description for NVM Express Base Specification 2.0 Changes Document

3 NVM Express Architecture

…

3.1.2.3 Discovery Controller

A Discovery controller only implements features related to Discovery Log Pages and does not implement I/O Queues, I/O commands, or expose namespaces. The functionality supported by the Discovery controller is defined in section 3.1.2.3.4.

If the Discovery subsystem provides a unique NQN (i.e., the NVM Subsystem NVMe Qualified Name (SUBNQN) field in that Discovery subsystem's Identify Controller data structure contains a unique NQN value), then that Discovery subsystem shall support both the unique NQN and the well-known Discovery Service NQN (i.e., nqn.2014-08.org.nvmexpress.discovery) being specified in the Connect command (refer to section 6.3) from the host.

If the Discovery subsystem does not provide a unique NQN (i.e., the SUBNQN field in that Discovery subsystem's Identify Controller data structure contains the well-known Discovery Service NQN), then that Discovery subsystem shall support the well-known Discovery Service NQN being specified in the Connect command from the host.

In the Connect command to a Discovery subsystem that provides a unique NQN, ~~T~~the host may use~~s~~ either of the following:

- the well-known Discovery Service NQN ~~(nqn.2014-08.org.nvmexpress.discovery)~~; or ~~in the Connect command (refer to section 6.3) to a Discovery Service.~~
- the unique NQN of that Discovery subsystem.

In the Connect command to a Discovery subsystem that does not provide a unique NQN, the host uses the well-known Discovery Service NQN.

The method that a host uses to obtain the NVMe Transport information necessary to connect to the well-known Discovery Service is implementation specific.

The Discovery Log Page provided by a Discovery controller contains one or more entries. Each entry specifies information necessary for the host to connect to an NVM subsystem. An entry may be associated with an NVM subsystem that exposes namespaces or a referral to another Discovery Service. There are no ordering requirements for log page entries within the Discovery Log Page.

…

5 Admin Command Set

…

5.16.1.23 Discovery Log Page (Log Identifier 70h)

…

Figure 264: Get Log Page – Discovery Log Page Entry

Bytes	Description
…	**…**
255:64	Reserved
511:256	**NVM Subsystem Qualified Name (SUBNQN):** NVMe Qualified Name (NQN) that uniquely identifies the NVM subsystem. Refer to section 4.4. For a Discovery ~~Service~~subsystem, if that Discovery subsystem has a unique NQN (i.e., the NVM Subsystem NVMe Qualified Name (SUBNQN) field in that Discovery subsystem's Identify Controller data structure contains a unique NQN value), then the value returned shall be that unique NQN. If the Discovery subsystem does not have a unique NQN, then the value returned shall be the well-known Discovery Service NQN (i.e., nqn.2014-08.org.nvmexpress.discovery).
767:512	**Transport Address (TRADDR):** Specifies the address of the NVM subsystem that may be used for a Connect command as an ASCII string. The Address Family field describes the reference for parsing this field. Refer to section 1.4.2 for ASCII string requirements. For the definition of this field, refer to the appropriate NVMe Transport binding specification.
…	**…**

…

5.17.2.1 Identify Controller data Structure (CNS 01h)

…

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

Bytes	I/O[1]	Admin[1]	Disc[1]	Description
…	…	…	…	**…**
767:564				Reserved
1023:768	M	M	R	**NVM Subsystem NVMe Qualified Name (SUBNQN):** This field specifies the NVM Subsystem NVMe Qualified Name as a UTF-8 null-terminated string. Refer to section 4.5 for the definition of NVMe Qualified Name. Support for this field is mandatory if the controller supports revision 1.2.1 or later as indicated in the Version property (refer to section 3.1.3.2). For a Discovery controller, if the Discovery subsystem containing the Discovery controller has a unique NQN, then this field shall be set to that unique NQN. If the Discovery subsystem containing the Discovery controller does not have a unique NQN, then this field shall be set to the well-known Discovery Service NQN (i.e., nqn.2014-08.org.nvmexpress.discovery).
1791:1024				Reserved
…	…	…	…	**…**

NOTES:

1. O/M/R definition: O = Optional, M = Mandatory, R = Reserved.
2. Mandatory for I/O controllers using a message-based transport. Reserved for I/O controllers using a memory-based transport.

…

8 Extended Capabilities

…

8.13.2 NVMe In-band Authentication

…

The Authentication and Security Requirements (AUTHREQ) field in the Connect response capsule (refer to Figure 382) indicates whether NVMe in-band authentication is required.

If one or more of the bits in the AUTHREQ field are set to ‘1’, then the controller requires that the host authenticate on that queue in order to proceed with Fabrics, Admin, and I/O commands. Authentication success is defined by the specific security protocol that is used for authentication. If any command other than Connect, Authentication Send, or Authentication Receive is received prior to authentication success, then the controller shall abort the command with Authentication Required status.

If all bits in the AUTHREQ field are cleared to ‘0’, then the controller does not require the host to authenticate, and the NVM subsystem shall not abort any command with a status value of Authentication Required.

If a Discovery subsystem provides a unique NQN (refer to section 3.1.2.3), then NVMe in-band authentication should be performed using that unique NQN (i.e., the well-known Discovery Service NQN should not be used). The host may connect to that Discovery subsystem using the well-known Discovery Service NQN (i.e., nqn.2014-08.org.nvmexpress.discovery) to determine if that Discovery subsystem provides a unique NQN. The connection using the well-known Discovery Service NQN may or may not require authentication. If the Discovery subsystem does provide a unique NQN, then the host may disconnect the connection to the well-known Discovery Service NQN and reconnect to that Discovery subsystem using the unique NQN. The connection using the unique NQN may or may not require authentication.

If NVMe in-band authentication succeeds, then any supported commands for the associated queue type may be processed.

The host may initiate a subsequent authentication transaction at any time for reauthentication purposes. Initiating reauthentication shall not invalidate a prior authentication. If the reauthentication transaction concludes with the controller sending an AUTH_Failure1 message (refer to section 8.13.4.2), then the controller shall terminate all commands with a status of Operation Denied and disconnect the NVMe over Fabrics connection. If the reauthentication transaction concludes with the host sending an AUTH_Failure2 message, then the host shall disconnect the NVMe over Fabrics connection.

…