



**Document Number: DSP0217**

**Date: 2009-08-04**

**Version: 2.0.0**

# **SMASH Implementation Requirements**

**Document Type: Specification**

**Document Status: DMTF Standard**

**Document Language: E**

**Copyright Notice**

Copyright © 2007, 2009 Distributed Management Task Force, Inc. (DMTF). All rights reserved.

DMTF is a not-for-profit association of industry members dedicated to promoting enterprise and systems management and interoperability. Members and non-members may reproduce DMTF specifications and documents, provided that correct attribution is given. As DMTF specifications may be revised from time to time, the particular version and release date should always be noted.

Implementation of certain elements of this standard or proposed standard may be subject to third party patent rights, including provisional patent rights (herein "patent rights"). DMTF makes no representations to users of the standard as to the existence of such rights, and is not responsible to recognize, disclose, or identify any or all such third party patent right, owners or claimants, nor for any incomplete or inaccurate identification or disclosure of such rights, owners or claimants. DMTF shall have no liability to any party, in any manner or circumstance, under any legal theory whatsoever, for failure to recognize, disclose, or identify any such third party patent rights, or for such party's reliance on the standard or incorporation thereof in its product, protocols or testing procedures. DMTF shall have no liability to any party implementing such standard, whether such implementation is foreseeable or not, nor to any patent owner or claimant, and shall have no liability or responsibility for costs or losses incurred if a standard is withdrawn or modified after publication, and shall be indemnified and held harmless by any party implementing the standard from any and all claims of infringement by a patent owner for such implementations.

For information about patents held by third-parties which have notified the DMTF that, in their opinion, such patent may relate to or impact implementations of DMTF standards, visit <http://www.dmtf.org/about/policies/disclosures.php>.

# CONTENTS

Foreword .....	5
Introduction .....	6
1 Scope .....	7
2 Normative References.....	7
2.1 Approved References .....	7
2.2 Other References.....	11
3 Terms and Definitions .....	11
4 Mandatory Specification Requirements .....	12
4.1 Mandatory Profile Requirements .....	12
4.2 Mandatory Protocol Requirements .....	12
5 Conditional Profile Specification Requirements .....	13
5.1 Base Server Profile .....	13
5.2 Boot Control Profile.....	13
5.3 Service Processor Profile .....	13
5.4 CLP Service Profile.....	13
5.5 CPU Profile .....	13
5.6 Device Tray Profile.....	14
5.7 DHCP Client Profile .....	14
5.8 DNS Client Profile.....	14
5.9 Ethernet Port Profile.....	14
5.10 Fan Profile.....	14
5.11 IP Interface Profile .....	14
5.12 Modular System Profile.....	14
5.13 Pass-through Module Profile .....	15
5.14 Physical Asset Profile .....	15
5.15 Power State Management Profile .....	15
5.16 Power Supply Profile.....	15
5.17 Record Log Profile .....	15
5.18 Role Based Authorization Profile .....	15
5.19 Sensors Profile.....	15
5.20 Shared Device Management Profile .....	16
5.21 Simple Identity Management Profile .....	16
5.22 SM CLP Admin Domain Profile.....	16
5.23 SMASH Collections Profile .....	16
5.24 Software Inventory Profile.....	16
5.25 Software Update Profile .....	16
5.26 SSH Service Profile .....	16
5.27 System Memory Profile.....	17
5.28 Telnet Service Profile.....	17
5.29 Text Console Redirection Profile .....	17
5.30 Watchdog Profile.....	17
5.31 KVM Redirection Profile.....	17
5.32 PCI Device Profile.....	17
5.33 OS Status Profile .....	18
5.34 Indicator LED Profile .....	18
5.35 Indications Profile.....	18
5.36 SMI-S Host Hardware Raid Controller Profile .....	18
6 Conditional Protocol Implementation Requirements.....	19
6.1 SM CLP Protocol Conditional Requirements.....	19
6.2 Management Protocol.....	19

7	Security Implementation Requirements .....	22
7.1	WS Management Protocol Specific Security Requirements.....	22
8	Discovery Requirements .....	25
8.1	Network Endpoint Discovery Stage .....	25
8.2	WS Management Access Point Discovery .....	25
	ANNEX A (informative) Change Log.....	27
	Bibliography .....	28

## Tables

Table 1 – WS-Transfer Operations .....	19
Table 2 – WS-Enumeration Operations .....	20
Table 3 – WS-Eventing Operations .....	20
Table 4 – WS-Eventing Message Security Recommendations .....	21
Table 6 – Operational Roles Supported.....	23
Table 7 – User Account Operations.....	24
Table 8 – Authentication Mechanisms .....	24
Table 9 – WS-Management IdentifyResponse Payload Elements .....	25

## Foreword

The *SMASH Implementation Requirements* (DSP0217) was prepared by the Server Management Working Group of the DMTF.

DMTF is a not-for-profit association of industry members dedicated to promoting enterprise and systems management and interoperability.

### **Acknowledgements**

The authors wish to acknowledge the following people.

Contributors:

- Aaron Merkin – IBM
- Jeff Hilland – HP

Participants from the DMTF Server Management Working Group:

- Jon Hass – Dell
- Khachatur Papanyan – Dell
- Radhakrishna Dasari – Dell
- Jeff Hilland – HP
- Aaron Merkin – IBM
- John Leung – Intel
- Joel Clark – Intel

## Introduction

This specification describes the conformance requirements for implementing the System Management Architecture for Server Hardware (SMASH) version 2.0.

1

# SMASH Implementation Requirements

## 2 1 Scope

3 This document specifies the requirements for implementing the System Management Architecture for  
4 Server Hardware (SMASH) version 2.0. This document specifies those requirements by defining which  
5 other DMTF specifications are required, conditional, and optional. The mandatory specifications to be  
6 implemented are defined in clause 4. The optional and conditional specifications are defined in clauses 5,  
7 6, 7, and 8.

## 8 2 Normative References

9 The following referenced documents are indispensable for the application of this document. For dated  
10 references, only the edition cited applies. For undated references, the latest edition of the referenced  
11 document (including any amendments) applies.

### 12 2.1 Approved References

13 DMTF DSP0214, *Server Management Command Line Protocol Specification, 1.0*,  
14 [http://www.dmtf.org/standards/published\\_documents/DSP0214\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP0214_1.0.pdf)

15 DMTF DSP0215, *Server Management Managed Element (SM ME) Specification, 1.0*,  
16 [http://www.dmtf.org/standards/published\\_documents/DSP0215\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP0215_1.0.pdf)

17 DMTF DSP0216, *SM CLP to CIM Common Mapping Specification, 1.0*,  
18 [http://www.dmtf.org/standards/published\\_documents/DSP0216\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP0216_1.0.pdf)

19 DMTF DSP0226, *Web Services for Management (WS Management), 1.0*,  
20 [http://www.dmtf.org/standards/published\\_documents/DSP0226\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP0226_1.0.pdf)

21 DMTF DSP0227, *WS-Management CIM Binding Specification, 1.0*,  
22 [http://www.dmtf.org/standards/published\\_documents/DSP0227\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP0227_1.0.pdf)

23 DMTF DSP0230, *WS-CIM Mapping Specification, 1.0*,  
24 [http://www.dmtf.org/standards/published\\_documents/DSP0230\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP0230_1.0.pdf)

25 DMTF DSP0800, *Base Server Profile SM CLP Command Mapping Specification, 1.0*,  
26 [http://www.dmtf.org/standards/published\\_documents/DSP0800\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP0800_1.0.pdf)

27 DMTF DSP0801, *CLP Service Profile SM CLP Command Mapping Specification, 1.0*,  
28 [http://www.dmtf.org/standards/published\\_documents/DSP0801\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP0801_1.0.pdf)

29 DMTF DSP0802, *SMASH Collections Profile SM CLP Command Mapping Specification, 1.0*,  
30 [http://www.dmtf.org/standards/published\\_documents/DSP0802\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP0802_1.0.pdf)

31 DMTF DSP0803, *SM CLP Admin Domain Profile SM CLP Command Mapping Specification, 1.0*,  
32 [http://www.dmtf.org/standards/published\\_documents/DSP0803\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP0803_1.0.pdf)

33 DMTF DSP0804, *Modular System Profile SM CLP Command Mapping Specification, 1.0*,  
34 [http://www.dmtf.org/standards/published\\_documents/DSP0804\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP0804_1.0.pdf)

35 DMTF DSP0805, *Sensors Profile SM CLP Command Mapping Specification, 1.0*,  
36 [http://www.dmtf.org/standards/published\\_documents/DSP0805\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP0805_1.0.pdf)

- 37 DMTF DSP0806, *Device Tray Profile SM CLP Command Mapping Specification, 1.0,*  
38 [http://www.dmtf.org/standards/published\\_documents/DSP0806\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP0806_1.0.pdf)
- 39 DMTF DSP0807, *Pass-Through Module Profile SM CLP Command Mapping Specification, 1.0,*  
40 [http://www.dmtf.org/standards/published\\_documents/DSP0807\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP0807_1.0.pdf)
- 41 DMTF DSP0808, *CPU Profile SM CLP Command Mapping Specification, 1.0,*  
42 [http://www.dmtf.org/standards/published\\_documents/DSP0808\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP0808_1.0.pdf)
- 43 DMTF DSP0809, *System Memory Profile SM CLP Command Mapping Specification, 1.0,*  
44 [http://www.dmtf.org/standards/published\\_documents/DSP0809\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP0809_1.0.pdf)
- 45 DMTF DSP0810, *Record Log Profile SM CLP Command Mapping Specification, 1.0,*  
46 [http://www.dmtf.org/standards/published\\_documents/DSP0810\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP0810_1.0.pdf)
- 47 DMTF DSP0811, *Simple Identity Management Profile SM CLP Command Mapping Specification, 1.0,*  
48 [http://www.dmtf.org/standards/published\\_documents/DSP0811\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP0811_1.0.pdf)
- 49 DMTF DSP0812, *Physical Asset Profile SM CLP Command Mapping Specification, 1.0,*  
50 [http://www.dmtf.org/standards/published\\_documents/DSP0812\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP0812_1.0.pdf)
- 51 DMTF DSP0813, *Boot Control Profile SM CLP Command Mapping Specification, 1.0,*  
52 [http://www.dmtf.org/standards/published\\_documents/DSP0813\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP0813_1.0.pdf)
- 53 DMTF DSP0814, *Fan Profile SM CLP Command Mapping Specification, 1.0,*  
54 [http://www.dmtf.org/standards/published\\_documents/DSP0814\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP0814_1.0.pdf)
- 55 DMTF DSP0815, *Ethernet Port Profile SM CLP Command Mapping Specification, 1.0,*  
56 [http://www.dmtf.org/standards/published\\_documents/DSP0815\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP0815_1.0.pdf)
- 57 DMTF DSP0817, *IP Interface Profile SM CLP Command Mapping Specification, 1.0,*  
58 [http://www.dmtf.org/standards/published\\_documents/DSP0817\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP0817_1.0.pdf)
- 59 DMTF DSP0818, *DHCP Client Profile SM CLP Command Mapping Specification, 1.0,*  
60 [http://www.dmtf.org/standards/published\\_documents/DSP0818\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP0818_1.0.pdf)
- 61 DMTF DSP0819, *DNS Client Profile SM CLP Command Mapping Specification, 1.0,*  
62 [http://www.dmtf.org/standards/published\\_documents/DSP0819\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP0819_1.0.pdf)
- 63 DMTF DSP0820, *Telnet Service Profile SM CLP Command Mapping Specification, 1.0,*  
64 [http://www.dmtf.org/standards/published\\_documents/DSP0820\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP0820_1.0.pdf)
- 65 DMTF DSP0821, *SSH Service Profile SM CLP Command Mapping Specification, 1.0,*  
66 [http://www.dmtf.org/standards/published\\_documents/DSP0821\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP0821_1.0.pdf)
- 67 DMTF DSP0822, *Power Supply Profile SM CLP Command Mapping Specification, 1.0,*  
68 [http://www.dmtf.org/standards/published\\_documents/DSP0822\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP0822_1.0.pdf)
- 69 DMTF DSP0823, *Power State Management Profile SM CLP Command Mapping Specification, 1.0,*  
70 [http://www.dmtf.org/standards/published\\_documents/DSP0823\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP0823_1.0.pdf)
- 71 DMTF DSP0824, *Service Processor Profile SM CLP Command Mapping Specification, 1.0,*  
72 [http://www.dmtf.org/standards/published\\_documents/DSP0824\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP0824_1.0.pdf)
- 73 DMTF DSP0825, *Shared Device Management Profile SM CLP Command Mapping Specification, 1.0,*  
74 [http://www.dmtf.org/standards/published\\_documents/DSP0825\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP0825_1.0.pdf)
- 75 DMTF DSP0826, *Software Inventory Profile SM CLP Command Mapping Specification, 1.0,*  
76 [http://www.dmtf.org/standards/published\\_documents/DSP0826\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP0826_1.0.pdf)



- 77 DMTF DSP0827, *Software Update Profile SM CLP Command Mapping Specification, 1.0,*  
78 [http://www.dmtf.org/standards/published\\_documents/DSP0827\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP0827_1.0.pdf)
- 79 DMTF DSP0828, *Text Console Redirection Profile SM CLP Command Mapping Specification, 1.0,*  
80 [http://www.dmtf.org/standards/published\\_documents/DSP0828\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP0828_1.0.pdf)
- 81 DMTF DSP0830, *Role Based Authorization Profile SM CLP Command Mapping Specification, 1.0,*  
82 [http://www.dmtf.org/standards/published\\_documents/DSP0830\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP0830_1.0.pdf)
- 83 DMTF DSP0831, *Platform Watchdog Profile SM CLP Command Mapping Specification, 1.0,*  
84 [http://www.dmtf.org/standards/published\\_documents/DSP0831\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP0831_1.0.pdf)
- 85 DMTF DSP0835, *Indicator LED Profile SM CLP Command Mapping Specification, 1.0,*  
86 [http://www.dmtf.org/standards/published\\_documents/DSP0835\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP0835_1.0.pdf)
- 87 DMTF DSP0836, *KVM Redirection Profile SM CLP Command Mapping Specification, 1.0,*  
88 [http://www.dmtf.org/standards/published\\_documents/DSP0836\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP0836_1.0.pdf)
- 89 DMTF DSP0838, *PCI Device Profile SM CLP Command Mapping Specification, 1.0,*  
90 [http://www.dmtf.org/standards/published\\_documents/DSP0838\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP0838_1.0.pdf)
- 91 DMTF DSP0842, *OS Status Profile SM CLP Command Mapping Specification, 1.0,*  
92 [http://www.dmtf.org/standards/published\\_documents/DSP0842\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP0842_1.0.pdf)
- 93 DMTF DSP1004, *Base Server Profile, 1.0,*  
94 [http://www.dmtf.org/standards/published\\_documents/DSP1004\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP1004_1.0.pdf)
- 95 DMTF DSP1005, *CLP Service Profile, 1.0,*  
96 [http://www.dmtf.org/standards/published\\_documents/DSP1005\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP1005_1.0.pdf)
- 97 DMTF DSP1006, *SMASH Collections Profile, 1.0,*  
98 [http://www.dmtf.org/standards/published\\_documents/DSP1006\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP1006_1.0.pdf)
- 99 DMTF DSP1007, *SM CLP Admin Domain Profile, 1.0,*  
100 [http://www.dmtf.org/standards/published\\_documents/DSP1007\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP1007_1.0.pdf)
- 101 DMTF DSP1008, *Modular System Profile, 1.0,*  
102 [http://www.dmtf.org/standards/published\\_documents/DSP1008\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP1008_1.0.pdf)
- 103 DMTF DSP1009, *Sensors Profile, 1.0,*  
104 [http://www.dmtf.org/standards/published\\_documents/DSP1009\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP1009_1.0.pdf)
- 105 DMTF DSP1010, *Record Log Profile, 1.0,*  
106 [http://www.dmtf.org/standards/published\\_documents/DSP1010\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP1010_1.0.pdf)
- 107 DMTF DSP1011, *Physical Asset Profile, 1.0,*  
108 [http://www.dmtf.org/standards/published\\_documents/DSP1011\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP1011_1.0.pdf)
- 109 DMTF DSP1012, *Boot Control Profile, 1.0,*  
110 [http://www.dmtf.org/standards/published\\_documents/DSP1012\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP1012_1.0.pdf)
- 111 DMTF DSP1013, *Fan Profile, 1.0,*  
112 [http://www.dmtf.org/standards/published\\_documents/DSP1013\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP1013_1.0.pdf)
- 113 DMTF DSP1014, *Ethernet Port Profile, 1.0,*  
114 [http://www.dmtf.org/standards/published\\_documents/DSP1014\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP1014_1.0.pdf)
- 115 DMTF DSP1015, *Power Supply Profile, 1.0,*  
116 [http://www.dmtf.org/standards/published\\_documents/DSP1015\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP1015_1.0.pdf)

- 117 DMTF DSP1016, *Telnet Service Profile, 1.0*,  
118 [http://www.dmtf.org/standards/published\\_documents/DSP1016\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP1016_1.0.pdf)
- 119 DMTF DSP1017, *SSH Service Profile, 1.0*,  
120 [http://www.dmtf.org/standards/published\\_documents/DSP1017\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP1017_1.0.pdf)
- 121 DMTF DSP1018, *Service Processor Profile, 1.0*,  
122 [http://www.dmtf.org/standards/published\\_documents/DSP1018\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP1018_1.0.pdf)
- 123 DMTF DSP1019, *Device Tray Profile, 1.0*,  
124 [http://www.dmtf.org/standards/published\\_documents/DSP1019\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP1019_1.0.pdf)
- 125 DMTF DSP1020, *Pass-Through Module Profile, 1.0*,  
126 [http://www.dmtf.org/standards/published\\_documents/DSP1020\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP1020_1.0.pdf)
- 127 DMTF DSP1021, *Shared Device Management Profile, 1.0*,  
128 [http://www.dmtf.org/standards/published\\_documents/DSP1021\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP1021_1.0.pdf)
- 129 DMTF DSP1022, *CPU Profile, 1.0*,  
130 [http://www.dmtf.org/standards/published\\_documents/DSP1022\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP1022_1.0.pdf)
- 131 DMTF DSP1023, *Software Inventory Profile, 1.0*,  
132 [http://www.dmtf.org/standards/published\\_documents/DSP1023\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP1023_1.0.pdf)
- 133 DMTF DSP1024, *Text Console Redirection Profile, 1.0*,  
134 [http://www.dmtf.org/standards/published\\_documents/DSP1024\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP1024_1.0.pdf)
- 135 DMTF DSP1025, *Software Update Profile, 1.0*,  
136 [http://www.dmtf.org/standards/published\\_documents/DSP1025\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP1025_1.0.pdf)
- 137 DMTF DSP1026, *System Memory Profile, 1.0*,  
138 [http://www.dmtf.org/standards/published\\_documents/DSP1026\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP1026_1.0.pdf)
- 139 DMTF DSP1027, *Power State Management Profile, 1.0*,  
140 [http://www.dmtf.org/standards/published\\_documents/DSP1027\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP1027_1.0.pdf)
- 141 DMTF DSP1029, *OS Status Profile, 1.0*,  
142 [http://www.dmtf.org/standards/published\\_documents/DSP1029\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP1029_1.0.pdf)
- 143 DMTF DSP1033, *Profile Registration Profile, 1.0*,  
144 [http://www.dmtf.org/standards/published\\_documents/DSP1033\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP1033_1.0.pdf)
- 145 DMTF DSP1034, *Simple Identity Management Profile, 1.0*,  
146 [http://www.dmtf.org/standards/published\\_documents/DSP1034\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP1034_1.0.pdf)
- 147 DMTF DSP1036, *IP Interface Profile, 1.0*,  
148 [http://www.dmtf.org/standards/published\\_documents/DSP1036\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP1036_1.0.pdf)
- 149 DMTF DSP1037, *DHCP Client Profile, 1.0*,  
150 [http://www.dmtf.org/standards/published\\_documents/DSP1037\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP1037_1.0.pdf)
- 151 DMTF DSP1038, *DNS Client Profile, 1.0*,  
152 [http://www.dmtf.org/standards/published\\_documents/DSP1038\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP1038_1.0.pdf)
- 153 DMTF DSP1039, *Role Based Authorization Profile, 1.0*,  
154 [http://www.dmtf.org/standards/published\\_documents/DSP1039\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP1039_1.0.pdf)
- 155 DMTF DSP1040, *Watchdog Profile, 1.0*,  
156 [http://www.dmtf.org/standards/published\\_documents/DSP1040\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP1040_1.0.pdf)

- 157 DMTF DSP1054, *Indications Profile, 1.0*,  
158 [http://www.dmtf.org/standards/published\\_documents/DSP1054\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP1054_1.0.pdf)
- 159 DMTF DSP1074, *Indicator LED Profile, 1.0*,  
160 [http://www.dmtf.org/standards/published\\_documents/DSP1074\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP1074_1.0.pdf)
- 161 DMTF DSP1075, *PCI Device Profile, 1.0*,  
162 [http://www.dmtf.org/standards/published\\_documents/DSP1075\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP1075_1.0.pdf)
- 163 DMTF DSP1076, *KVM Redirection Profile, 1.0*,  
164 [http://www.dmtf.org/standards/published\\_documents/DSP1076\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP1076_1.0.pdf)
- 165 DMTF DSP8007, *Platform Message Registry, 1.0*,  
166 [http://www.dmtf.org/standards/published\\_documents/DSP8007\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP8007_1.0.pdf)
- 167 DMTF DSP8039, SMASH XML Schema, 1.0, <http://schemas.dmtf.org/wbem/smash/1/dsp8039.xsd>
- 168 IETF RFC 2246, T. Dierks et al., *The TLS Protocol Version 1.0*, <http://www.ietf.org/rfc/rfc2246.txt>
- 169 IETF RFC 4106, J. Viega and D. McGrew, *The Use of Galois/Counter Mode (GCM) in IPsec*  
170 *Encapsulating Security Payload (ESP)*, <http://www.ietf.org/rfc/rfc4106.txt>
- 171 IETF RFC 4301, S. Kent, *Security Architecture for the Internet Protocol*, <http://www.ietf.org/rfc/rfc4301.txt>
- 172 IETF RFC 4303, S. Kent, *IP Encapsulating Security Payload (ESP)*, <http://www.ietf.org/rfc/rfc4303.txt>
- 173 SNIA, *Storage Management Initiative Specification (SMI-S) 1.3.0*,  
174 [http://www.snia.org/tech\\_activities/standards/curr\\_standards/smi](http://www.snia.org/tech_activities/standards/curr_standards/smi)

## 175 **2.2 Other References**

- 176 ISO/IEC Directives, Part 2, *Rules for the structure and drafting of International Standards*,  
177 <http://isotc.iso.org/livelink/livelink.exe?func=ll&objId=4230456&objAction=browse&sort=subtype>

## 178 **3 Terms and Definitions**

179 For the purposes of this document, the following terms and definitions apply.

### 180 **3.1**

#### 181 **can**

182 used for statements of possibility and capability, whether material, physical, or causal

### 183 **3.2**

#### 184 **cannot**

185 used for statements of possibility and capability, whether material, physical, or causal

### 186 **3.3**

#### 187 **conditional**

188 indicates requirements to be followed strictly in order to conform to the document when the specified  
189 conditions are met

### 190 **3.4**

#### 191 **mandatory**

192 indicates requirements to be followed strictly in order to conform to the document and from which no  
193 deviation is permitted

- 194 **3.5**  
195 **may**  
196 indicates a course of action permissible within the limits of the document
- 197 **3.6**  
198 **need not**  
199 indicates a course of action permissible within the limits of the document
- 200 **3.7**  
201 **optional**  
202 indicates a course of action permissible within the limits of the document
- 203 **3.8**  
204 **shall**  
205 indicates requirements to be followed strictly in order to conform to the document and from which no  
206 deviation is permitted
- 207 **3.9**  
208 **shall not**  
209 indicates requirements to be followed in order to conform to the document and from which no deviation is  
210 permitted
- 211 **3.10**  
212 **should**  
213 indicates that among several possibilities, one is recommended as particularly suitable, without  
214 mentioning or excluding others, or that a certain course of action is preferred but not necessarily required
- 215 **3.11**  
216 **should not**  
217 indicates that a certain possibility or course of action is deprecated but not prohibited

## 218 **4 Mandatory Specification Requirements**

219 This section lists mandatory profiles and protocols that are required for this specification.

### 220 **4.1 Mandatory Profile Requirements**

221 At least one of the following profiles shall be implemented:

- 222 • DMTF [DSP1004](#), *Base Server Profile*, 1.0
- 223 • DMTF [DSP1018](#), *Service Processor Profile*, 1.0
- 224 • DMTF [DSP1008](#), *Modular System Profile*, 1.0

### 225 **4.2 Mandatory Protocol Requirements**

226 At least one of the following protocols shall be implemented:

- 227 • DMTF [DSP0214](#), *Server Management Command Line Protocol Specification*, 1.0
- 228 • DMTF [DSP0226](#), *Web Services for Management*, 1.0

## 229 5 Conditional Profile Specification Requirements

230 This section details the requirements for profiles and their associated mapping specifications.  
231 Implementations may expose different sets of Profiles via the protocols. This implies that a Mapping  
232 Specification for a Profile is only required if the Profile is exposed through the CLP irrespective of whether  
233 or not it is exposed via WS Management.

### 234 5.1 Base Server Profile

235 The [Base Server Profile](#) may be implemented. If the *Base Server Profile* is implemented, the following  
236 requirements shall be met:

237 If [DSP0214](#), the *Server Management Command Line Protocol Specification*, is implemented, the  
238 optional behavior of implementing the [SMASH Collections Profile](#) specified in the *Base Server Profile*  
239 shall be implemented. The [Base Server Profile SM CLP Command Mapping Specification](#) shall be  
240 implemented.

### 241 5.2 Boot Control Profile

242 The [Boot Control Profile](#) may be implemented. If the *Boot Control Profile* is implemented, the following  
243 requirements shall be met:

244 If [DSP0214](#), the *Server Management Command Line Protocol Specification*, is implemented and the  
245 profile is exposed using the SM CLP, the [Boot Control Profile SM CLP Command Mapping](#)  
246 [Specification](#) shall be implemented.

### 247 5.3 Service Processor Profile

248 The [Service Processor Profile](#) may be implemented. If the *Service Processor Profile* is implemented, the  
249 following requirements shall be met:

250 If [DSP0214](#), the *Server Management Command Line Protocol Specification*, is implemented and the  
251 profile is exposed using the SM CLP, the optional behavior of implementing the [SMASH Collections](#)  
252 [Profile](#) specified in the *Service Processor Profile* shall be implemented. The [Service Processor](#)  
253 [Profile SM CLP Command Mapping Specification](#) shall be implemented.

### 254 5.4 CLP Service Profile

255 If [DSP0214](#), the *Server Management Command Line Protocol Specification*, is implemented and the  
256 profile is exposed using the SM CLP, the [CLP Service Profile](#) shall be implemented.

257 Either the optional behavior of implementing the [SSH Service Profile](#) specified in the *CLP Service Profile*  
258 or the optional behavior of implementing the [Telnet Service Profile](#) specified in the *CLP Service Profile*  
259 should be implemented. The [CLP Service Profile SM CLP Command Mapping Specification](#) shall be  
260 implemented.

### 261 5.5 CPU Profile

262 The [CPU Profile](#) may be implemented. If the *CPU Profile* is implemented and the profile is exposed using  
263 the SM CLP, the following requirements shall be met:

264 If [DSP0214](#), the *Server Management Command Line Protocol Specification*, is implemented, the  
265 [CPU Profile SM CLP Command Mapping Specification](#) shall be implemented.

## 266 5.6 Device Tray Profile

267 The [Device Tray Profile](#) may be implemented. If the *Device Tray Profile* is implemented and the profile is  
268 exposed using the SM CLP, the following requirements shall be met:

269 If [DSP0214](#), the *Server Management Command Line Protocol Specification*, is implemented, the  
270 [Device Tray Profile SM CLP Command Mapping Specification](#) shall be implemented.

## 271 5.7 DHCP Client Profile

272 The [DHCP Client Profile](#) may be implemented. If the *DHCP Client Profile* is implemented and the profile is  
273 exposed using the SM CLP, the following requirements shall be met:

274 If [DSP0214](#), the *Server Management Command Line Protocol Specification*, is implemented, the  
275 [DHCP Client Profile SM CLP Command Mapping Specification](#) shall be implemented.

## 276 5.8 DNS Client Profile

277 The [DNS Client Profile](#) may be implemented. If the *DNS Client Profile* is implemented and the profile is  
278 exposed using the SM CLP, the following requirements shall be met:

279 If [DSP0214](#), the *Server Management Command Line Protocol Specification*, is implemented, the  
280 [DNS Client Profile SM CLP Command Mapping Specification](#) shall be implemented.

## 281 5.9 Ethernet Port Profile

282 The [Ethernet Port Profile](#) may be implemented. If the *Ethernet Port Profile* is implemented and the profile  
283 is exposed using the SM CLP, the following requirements shall be met:

284 If [DSP0214](#), the *Server Management Command Line Protocol Specification*, is implemented, the  
285 [Ethernet Port Profile SM CLP Command Mapping Specification](#) shall be implemented.

## 286 5.10 Fan Profile

287 The [Fan Profile](#) may be implemented. If the *Fan Profile* is implemented and the profile is exposed using  
288 the SM CLP, the following requirements shall be met:

289 If [DSP0214](#), the *Server Management Command Line Protocol Specification*, is implemented, the [Fan](#)  
290 [Profile SM CLP Command Mapping Specification](#) shall be implemented.

## 291 5.11 IP Interface Profile

292 The [IP Interface Profile](#) may be implemented. If the *IP Interface Profile* is implemented and the profile is  
293 exposed using the SM CLP, the following requirements shall be met:

294 If [DSP0214](#), the *Server Management Command Line Protocol Specification*, is implemented, the  
295 [IP Interface Profile SM CLP Command Mapping Specification](#) shall be implemented.

## 296 5.12 Modular System Profile

297 The [Modular System Profile](#) may be implemented. If the *Modular System Profile* is implemented and the  
298 profile is exposed using the SM CLP, the following requirements shall be met:

299 If [DSP0214](#), the *Server Management Command Line Protocol Specification*, is implemented, the  
300 [Modular System Profile SM CLP Command Mapping Specification](#) shall be implemented.

### 301 5.13 Pass-through Module Profile

302 The [Pass-through Module Profile](#) may be implemented. If the *Pass-through Module Profile* is  
303 implemented and the profile is exposed using the SM CLP, the following requirements shall be met:

304 If [DSP0214](#), the *Server Management Command Line Protocol Specification*, is implemented, the  
305 [Pass-through Module Profile SM CLP Command Mapping Specification](#) shall be implemented.

### 306 5.14 Physical Asset Profile

307 The [Physical Asset Profile](#) may be implemented. If the *Physical Asset Profile* is implemented and the  
308 profile is exposed using the SM CLP, the following requirements shall be met:

309 If [DSP0214](#), the *Server Management Command Line Protocol Specification*, is implemented, the  
310 [Physical Asset Profile SM CLP Command Mapping Specification](#) shall be implemented.

### 311 5.15 Power State Management Profile

312 The [Power State Management Profile](#) may be implemented. If the *Power State Management Profile* is  
313 implemented and the profile is exposed using the SM CLP, the following requirements shall be met:

314 If [DSP0214](#), the *Server Management Command Line Protocol Specification*, is implemented, the  
315 [Power State Management Profile SM CLP Command Mapping Specification](#) shall be implemented.

### 316 5.16 Power Supply Profile

317 The [Power Supply Profile](#) may be implemented. If the *Power Supply Profile* is implemented and the  
318 profile is exposed using the SM CLP, the following requirements shall be met:

319 If [DSP0214](#), the *Server Management Command Line Protocol Specification*, is implemented, the  
320 [Power Supply Profile SM CLP Command Mapping Specification](#) shall be implemented.

### 321 5.17 Record Log Profile

322 The [Record Log Profile](#) may be implemented. If the *Record Log Profile* is implemented and the profile is  
323 exposed using the SM CLP, the following requirements shall be met:

324 If [DSP0214](#), the *Server Management Command Line Protocol Specification*, is implemented, the  
325 [Record Log Profile SM CLP Command Mapping Specification](#) shall be implemented.

### 326 5.18 Role Based Authorization Profile

327 The [Role Based Authorization Profile](#) may be implemented. If the *Role Based Authorization Profile* is  
328 implemented and the profile is exposed using the SM CLP, the following requirements shall be met:

329 If [DSP0214](#), the *Server Management Command Line Protocol Specification*, is implemented, the  
330 [Role Based Authorization Profile SM CLP Command Mapping Specification](#) shall be implemented.

### 331 5.19 Sensors Profile

332 The [Sensors Profile](#) may be implemented. If the *Sensors Profile* is implemented and the profile is  
333 exposed using the SM CLP, the following requirements shall be met:

334 If [DSP0214](#), the *Server Management Command Line Protocol Specification*, is implemented, the  
335 [Sensors Profile SM CLP Command Mapping Specification](#) shall be implemented.

## 336 5.20 Shared Device Management Profile

337 The [Shared Device Management Profile](#) may be implemented. If the *Shared Device Management Profile*  
338 is implemented and the profile is exposed using the SM CLP, the following requirements shall be met:

339 If [DSP0214](#), the *Server Management Command Line Protocol Specification*, is implemented, the  
340 [Shared Device Management Profile SM CLP Command Mapping Specification](#) shall be  
341 implemented.

## 342 5.21 Simple Identity Management Profile

343 The [Simple Identity Management Profile](#) may be implemented. If the *Simple Identity Management Profile*  
344 is implemented and the profile is exposed using the SM CLP, the following requirements shall be met:

345 If [DSP0214](#), the *Server Management Command Line Protocol Specification*, is implemented, the  
346 [Simple Identity Management Profile SM CLP Command Mapping Specification](#) shall be  
347 implemented.

## 348 5.22 SM CLP Admin Domain Profile

349 If [DSP0214](#), the *Server Management Command Line Protocol Specification*, is implemented and the  
350 profile is exposed using the SM CLP, the [SM CLP Admin Domain Profile SM CLP Command Mapping](#)  
351 [Specification](#) shall be implemented.

## 352 5.23 SMASH Collections Profile

353 If [DSP0214](#), the *Server Management Command Line Protocol Specification*, is implemented and the  
354 profile is exposed using the SM CLP, the [SMASH Collections Profile SM CLP Command Mapping](#)  
355 [Specification](#) shall be implemented.

## 356 5.24 Software Inventory Profile

357 The [Software Inventory Profile](#) may be implemented. If the *Software Inventory Profile* is implemented and  
358 the profile is exposed using the SM CLP, the following requirements shall be met:

359 If [DSP0214](#), the *Server Management Command Line Protocol Specification*, is implemented, the  
360 [Software Inventory Profile SM CLP Command Mapping Specification](#) shall be implemented.

## 361 5.25 Software Update Profile

362 The [Software Update Profile](#) may be implemented. If the *Software Update Profile* is implemented and the  
363 profile is exposed using the SM CLP, the following requirements shall be met:

364 If [DSP0214](#), the *Server Management Command Line Protocol Specification*, is implemented, the  
365 [Software Update Profile SM CLP Command Mapping Specification](#) shall be implemented.

## 366 5.26 SSH Service Profile

367 The [SSH Service Profile](#) may be implemented. If the *SSH Service Profile* is implemented and the profile is  
368 exposed using the SM CLP, the following requirements shall be met:

369 If [DSP0214](#), the *Server Management Command Line Protocol Specification*, is implemented, the  
370 [SSH Service Profile SM CLP Command Mapping Specification](#) shall be implemented.



## 371 5.27 System Memory Profile

372 The [System Memory Profile](#) may be implemented. If the *System Memory Profile* is implemented and the  
373 profile is exposed using the SM CLP, the following requirements shall be met:

374 If [DSP0214](#), the *Server Management Command Line Protocol Specification*, is implemented, the  
375 [System Memory Profile SM CLP Command Mapping Specification](#) shall be implemented.

## 376 5.28 Telnet Service Profile

377 The [Telnet Service Profile](#) may be implemented. If the *Telnet Service Profile* is implemented and the  
378 profile is exposed using the SM CLP, the following requirements shall be met:

379 If [DSP0214](#), the *Server Management Command Line Protocol Specification*, is implemented, the  
380 [Telnet Service Profile SM CLP Command Mapping Specification](#) shall be implemented.

## 381 5.29 Text Console Redirection Profile

382 The [Text Console Redirection Profile](#) may be implemented. If the *Text Console Redirection Profile* is  
383 implemented, the following requirements shall be met:

384 If [DSP0214](#), the *Server Management Command Line Protocol Specification*, is implemented and the  
385 profile is exposed using the SM CLP, the [Text Console Redirection Profile SM CLP Command  
386 Mapping Specification](#) shall be implemented.

## 387 5.30 Platform Watchdog Profile

388 The [Platform Watchdog Profile](#) may be implemented. If the *Platform Watchdog Profile* is implemented, the  
389 following requirements shall be met:

390 If [DSP0214](#), the *Server Management Command Line Protocol Specification*, is implemented and the  
391 profile is exposed using the SM CLP, the [Platform Watchdog Profile SM CLP Command Mapping  
392 Specification](#) shall be implemented.

## 393 5.31 KVM Redirection Profile

394 The [KVM Redirection Profile](#) may be implemented. If the *KVM Redirection Profile* is implemented, the  
395 following requirements shall be met:

396 If [DSP0214](#), the *Server Management Command Line Protocol Specification*, is implemented and the  
397 profile is exposed using the SM CLP, the [KVM Redirection Profile SM CLP Command Mapping  
398 Specification](#) shall be implemented.

## 399 5.32 PCI Device Profile

400 The [PCI Device Profile](#) may be implemented. If the *PCI Device Profile* is implemented, the following  
401 requirements shall be met:

402 If [DSP0214](#), the *Server Management Command Line Protocol Specification*, is implemented and the  
403 profile is exposed using the SM CLP, the [PCI Device Profile SM CLP Command Mapping  
404 Specification](#) shall be implemented.

### 405 5.33 OS Status Profile

406 The [OS Status Profile](#) may be implemented. If the *OS Status Profile* is implemented, the following  
407 requirements shall be met:

408 If [DSP0214](#), the *Server Management Command Line Protocol Specification*, is implemented and the  
409 profile is exposed using the SM CLP, the [OS Status Profile SM CLP Command Mapping](#)  
410 [Specification](#) shall be implemented.

### 411 5.34 Indicator LED Profile

412 The [Indicator LED Profile](#) may be implemented. If the *Indicator LED Profile* is implemented, the following  
413 requirements shall be met:

414 If [DSP0214](#), the *Server Management Command Line Protocol Specification*, is implemented and the  
415 profile is exposed using the SM CLP, the [Indicator LED Profile SM CLP Command Mapping](#)  
416 [Specification](#) shall be implemented.

### 417 5.35 Indications Profile

418 The [Indications Profile](#) may be implemented.

419 If [DSP0226](#), *Web Services for Management Specification* is implemented, the following requirements  
420 should be met:

- 421 • The *Indications Profile* ([DSP1054](#)) should be implemented.
- 422 • An instance of concrete subclass of CIM\_Indication should be the payload of WS-Event  
423 Delivery message. If an instance of CIM\_AlertIndication is used as a payload for WS-Event  
424 Delivery message, then the contents of the instance should be from [DSP8007](#), the *Platform*  
425 *Message Registry*.
- 426 • Any vendor-specific messages that are formulated should be from a published message registry  
427 with the owning entity set to other than the DMTF.

### 428 5.36 SMI-S Host Hardware Raid Controller Profile

429 The Host Hardware Raid Controller Profile (HHR Controller Profile) from the *Storage Management*  
430 *Initiative Specification (SMI-S)* may be implemented. If HHR Controller Profile is implemented, the  
431 following requirements shall be met:

- 432 • SMI-S Host Hardware Raid Profile from the *Storage Management Initiative Specification* shall  
433 not be implemented. The scoping class of the SMI-S HHR Controller profile shall be the central  
434 class of [DSP1018](#), (*Service Processor Profile*), [DSP1008](#) (*Modular System Profile*), or  
435 [DSP1004](#) (*Base Server Profile*).
- 436 • HHR Controller Profile and all the HHR Controller Profile referenced profiles shall implement  
437 [DSP1033](#) to advertise profile registration and shall not implement the SMI-S Server Profile from  
438 the *Storage Management Initiative Specification*.
- 439 • HHR Controller Profile and all the HHR Controller Profile referenced profiles may not implement  
440 mandatory indications. HHR Controller Profile and all the HHR Controller Profile referenced  
441 profiles may not implement the mandatory SMI-S Indication Profile from the *Storage*  
442 *Management Initiative Specification*.

443 **6 Conditional Protocol Implementation Requirements**

444 A SMASH-compliant implementation shall use a CIM-based data model for representing managed  
 445 resources and services. This section describes the Management Protocol and Transport Protocol  
 446 requirements for a SMASH implementation.

447 **6.1 SM CLP Protocol Conditional Requirements**

448 If [DSP0214](#), the *Server Management Command Line Protocol Specification*, is implemented, the following  
 449 requirements shall be met:

- 450 • [DSP0216](#), the *SM CLP to CIM Common Mapping Specification*, shall be implemented.
- 451 • [DSP0215](#), the *Server Management Managed Element Addressing Specification*, shall be  
 452 implemented.
- 453 • [DSP1005](#), the *CLP Service Profile*, shall be implemented.

454 **6.2 Management Protocol**

455 If [DSP0226](#), the *Web Services for Management Specification*, is implemented, the following requirements  
 456 shall be met:

- 457 • [DSP0227](#), the *WS-Management – CIM Binding Specification*, shall be implemented.
- 458 • [DSP0230](#), the *WS-CIM Mapping Specification*, shall be implemented.
- 459 • Implementations shall not support bindings to the protocol other than that specified in [DSP0227](#).

460 **6.2.1 XML Namespaces**

461 The following URI identifies an XML namespace that contains SMASH-specific XML definitions:

462 (1) `http://schemas.dmtf.org/wbem/smash/1`

463 Note that the schema location URL is <http://schemas.dmtf.org/wbem/smash/1/dsp8039.xsd>

464 **6.2.2 WS-Transfer**

465 It is mandatory for implementations to support WS-Transfer as described in section 4 of [DSP0226](#).  
 466 Table 1 defines support for WS-Transfer operations and their respective requirements.

467 **Table 1 – WS-Transfer Operations**

Operation	Requirement	Notes
Get	Mandatory	This operation retrieves resource representations. Implementations shall support the Get operation. Profiles require GetInstance support.
Put	Conditional	If a resource can be updated, the service shall support the Put operation. If an implemented profile requires ModifyInstance support, the Put operation shall be supported.
Create	Conditional	This operation creates resource instances. If an implemented profile requires CreateInstance support, the Create operation shall be supported.
Delete	Conditional	This operation deletes resources. If an implemented profile requires DeleteInstance support, the Delete operation shall be supported.

### 468 6.2.3 WS-Enumeration

469 It is mandatory for implementations to support WS-Enumeration as described in section 5 of [DSP0226](#).  
 470 Table 2 defines support for WS-Enumeration operations and their respective requirements.

471 **Table 2 – WS-Enumeration Operations**

Operation	Requirement	Messages
Enumerate	Mandatory	This operation is used to initiate an enumeration and receive an enumeration context.
Pull	Mandatory	This operation is used to pull a sequence of elements of a resource.
Renew	Optional	See Rule R5.1-4 in <a href="#">DSP0226</a> . Implementation of this operation is not recommended.
GetStatus	Optional	See Rule R5.1-4 in <a href="#">DSP0226</a> . Implementation of this operation is not recommended.
Release	Mandatory	This operation is used to release an enumeration context.
EnumerationEnd	Optional	See Rule R5.1-4 in <a href="#">DSP0226</a> . Implementation of this operation is not recommended.

472 It is recommended that the wsman:OptimizeEnumeration option be implemented as a child element of the  
 473 wsen:Enumerate element. Refer to section 5.2.3 of [DSP0226](#) for details. The service must accept the  
 474 element, but it does not have to honor it, as described in Rule R5.2.3-1 of [DSP0226](#).

475 It is optional for implementations to support the generic enumeration operations that are described in  
 476 clause 15.1 of [DSP0227](#), except the WS-Management equivalent of EnumerateInstances specified in  
 477 clause 15.1.5, which is mandatory as indicated in Table 2.

### 478 6.2.4 WS-Eventing

479 Support for WS-Eventing is conditional. A service advertising conformance to the Indications Profile shall  
 480 support WS-Eventing as described in clause 10 of [DSP0226](#) and further constrained by the definition  
 481 described in this section. Table 3 defines support for WS-Eventing operations and their respective  
 482 requirements.

483 **Table 3 – WS-Eventing Operations**

Operation	Requirement	Notes
Subscribe	Mandatory	
Renew	Mandatory	
Unsubscribe	Mandatory	
SubscriptionEnd	Optional	
GetStatus	Optional	See Rule R7.3-1 in <a href="#">DSP0226</a> . Implementation of this operation is not recommended.

484 **6.2.4.1 WS-Eventing Messaging Security**

485 For WS-Eventing the messaging security recommendations defined in Table 4 should be followed.

486 **Table 4 – WS-Eventing Message Security Recommendations**

Plane	WS-Eventing Message	Recommended Security Class	Security Principal Requiring Authentication
Control	wse:Subscribe	Class B (as defined in Section 7), because it can carry sensitive information	Subscriber
	wse:Renew	Class B (as defined in Section 7), because it can carry sensitive information	Subscriber
	wse:SubscriptionEnd	Class B (as defined in Section 7), because it can carry sensitive information	Subscriber
	wse:Unsubscribe	Class B (as defined in Section 7), because it can carry sensitive information	Subscriber
Delivery	wse:Delivery (Push)	Class A or B (as defined in Section 7); B for sensitive information or for more compute-intensive information	MAP, but not necessarily with its own credentials
	wse:Delivery (PushWithAck)	Class A or B (as defined in Section 7); B for sensitive information	MAP, but not necessarily with its own credentials
	wse:Delivery (Batched)	Class A or B (as defined in Section 7); B for sensitive information	MAP, but not necessarily with its own credentials
	wsen:Pull (Pull delivery)	Class A or B (as defined in Section 7); B for sensitive information	Subscriber
	Ack of delivery (on a separate connection)	Class A (as defined in Section 7)	Subscriber

487 **6.2.4.2 WS-Eventing Delivery Mode**

488 [DSP0226](#) defines four standard delivery modes (Push Mode, PushWithAck Mode, Batched Delivery Mode, and Pull Delivery Mode). Two of these delivery modes apply to SMASH as follows:

- 490 • Implementations shall support WS-Eventing Push Mode as described in section 7.2.10 of [DSP0226](#).
- 491
- 492 • Implementations should support WS-Eventing PushWithAck Mode as described in section 7.2.11 of [DSP0226](#).
- 493

494 **6.2.4.3 Eventing Source Port**

495 Implementations shall use the well known transport ports for eventing.

496 **6.2.4.4 Subscription-Related Property Definition Guidance**

497 The PersistenceType property in a CIM\_ListenerDestination instance created internally in response to wse:Subscribe should be set to 3 (Transient).

498

499 The value for the FailureTriggerTimeInterval property on the CIM\_IndicationSubscription or  
500 CIM\_FilterCollectionSubscription instance created internally in response to wse:Subscribe should be set  
501 to 30 seconds.

## 502 6.2.5 Transport Protocol

503 Implementations shall use HTTP 1.1 as the SOAP transport for [DSP0226](#). For detailed information about  
504 the transport protocol required, refer to the *Systems Management Architecture for Server Hardware White*  
505 *Paper* ([DSP2001](#)).

### 506 6.2.5.1 Transport TCP Port Requirements

507 Implementations shall support the IANA-defined system ports for product deployment, but may listen on  
508 other ports.

- 509 • Web Services Protocol Ports shall be supported on the following transport ports and shall be  
510 transport specific:
  - 511 – HTTP
  - 512 – HTTPS
- 513 • Support for the following sideband DMTF Web Services Protocol Ports is optional:
  - 514 – OOB-WS-HTTP
    - 515 • TCP Port 623
  - 516 – OOB-WS-HTTPS
    - 517 • TCP Port 664

## 518 7 Security Implementation Requirements

519 This section describes transport requirements, roles and authorization, user account management, and  
520 authentication.

### 521 7.1 WS Management Protocol Specific Security Requirements

522 If [DSP0226](#), the *Web Services for Management Specification*, is implemented, the requirements specified  
523 in this section shall be met.

#### 524 7.1.1 Transport Requirements

525 SMASH defines two security classes for HTTP 1.1 transport:

- 526 1) **Class A:** The security class A requires HTTP digest authentication for the user authentication.  
527 For this class, no encryption capabilities are required beyond the encryption of the password  
528 during the digest authentication exchange. If security Class A is supported, implementations  
529 should support MD5 or SHA-1 as the cryptographic algorithm.
  - 530 • **String = "HTTP\_DIGEST"**
    - 531 – URI = <http://schemas.dmtf.org/wbem/wsman/1/wsman/secprofile/http/digest>

532 2) **Class B:** This class defines three security profiles that are based on either TLS or IPsec with  
 533 specifically selected modes and cryptographic algorithms. For class B compliance, the support  
 534 for at least one of the following security profiles is mandatory:

- 535 • **String = “HTTP\_TLS\_1”**  
 536 – URI = http://schemas.dmtf.org/wbem/wsman/1/wsman/secprofile/https/digest
- 537 • **String = “HTTP\_TLS\_2”**  
 538 – URI = http://schemas.dmtf.org/wbem/wsman/1/wsman/secprofile/https/basic
- 539 • **String = “HTTP\_IPSEC”**  
 540 – URI = http://schemas.dmtf.org/wbem/wsman/1/wsman/secprofile/http/digest/ipsec

541 A SMASH implementation shall support at least one of the preceding security classes. It is recommended  
 542 that a SMASH implementation be Class B compliant for privacy/confidentiality and additional security.

543 Refer to 6.2.4.1 for WS-Eventing security requirements.

### 544 7.1.2 Cryptographic Algorithms and Cipher Suites

545 Table 5 lists the required cryptographic algorithms or cipher suites for the security profiles mentioned in  
 546 this section.

547 **Table 5- Required Cryptographic Algorithms or Cipher Suites**

Security Profile	Required Algorithm(s) or Cipher suite	Notes
“HTTP_DIGEST”	HMAC-MD5 or HMAC-SHA1	
“HTTP_TLS_1”	TLS_RSA_WITH_AES_128_CBC_SHA	TLS version 1.0 Refer to <a href="#">RFC 2246</a> .
“HTTP_TLS_2”	TLS_RSA_WITH_AES_128_CBC_SHA	TLS version 1.0 Refer to <a href="#">RFC 2246</a> .
“HTTP_IPSEC”	AES-GCM (key size: 128 bits, ICV or Digest len: 16 B) or AES-CBC (Key size: 128 bits) with HMAC-SHA1-96	Refer to <a href="#">RFC 4301</a> , <a href="#">RFC 4303</a> , and <a href="#">RFC 4106</a> .

### 548 7.1.3 Roles and Authorization

549 Table 6 outlines the Operational Roles supported by implementations and the respective requirements.

550 **Table 6 – Operational Roles Supported**

Operational Role	Requirement	Notes
Read-only User	Mandatory	
Operator	Optional	
Administrator	Mandatory	

551 A SMASH-compliant service should support the administrator and read-only roles. An implementation  
 552 may support the operator roles.

### 553 7.1.4 User Account Management

554 The authentication and authorization mechanisms defined are tied with user account management.  
 555 Implementations should support a role-based authorization model.

556 Each user should have the ability to modify its own account credentials. An account in the administrator  
 557 role should be able to perform account management for all users. Table 7 outlines the operations  
 558 supported for user account management and the respective requirements.

559

**Table 7 – User Account Operations**

Operation	Requirement	Notes
Create an account	Optional	Recommended for the administrator role
Delete an account	Optional	Recommended for the administrator role
Enable an account	Optional	
Disable an account	Optional	
Modify the privileges of an account	Optional	
Modify the password of an account	Conditional	Based on implementation of the Simple Identity Management Profile. Recommended for all roles
Change the role of an account	Optional	
Create a group of accounts	Optional	
Delete a group of accounts	Optional	
Add an account to a group	Optional	
Remove an account from a group	Optional	
Change the role of a group	Optional	
Modify the privileges of a group	Optional	
Change the associations of roles and accounts	Optional	Recommended for the administrator role

560 The modifications of privileges include the changing of bindings between accounts or groups and roles.  
 561 The privileges defined for SMASH 2.0 are static privileges.

### 562 7.1.5 Authentication Mechanisms

563 Implementations shall support one or two levels of authentication.

564 Table 8 outlines requirements for the three types of authentication mechanisms supported by SMASH 2.0  
 565 implementations.

566

**Table 8 – Authentication Mechanisms**

Authentication Mechanisms	Requirement	Notes
Machine-Level	Optional	Mandatory for class B security compliance
User-Level	Mandatory	At a minimum
Third-Party	Optional	



## 567 8 Discovery Requirements

568 Multiple discovery stages are required to accumulate the necessary information from the managed  
 569 system. This section defines the implementation requirements of the stages involved in discovering  
 570 managed systems and their management capabilities.

### 571 8.1 Network Endpoint Discovery Stage

572 The *SMASH White Paper* ([DSP2001](#)) describes endpoint discovery methods. A SMASH 2.0 compliant  
 573 implementation need not support any of the described methods.

### 574 8.2 WS Management Access Point Discovery

575 If [DSP0226](#), the *Web Services for Management Specification*, is implemented, the requirements specified  
 576 in this section shall be met.

#### 577 8.2.1 WS-Management Identify Method

578 Refer to section 8 of [DSP0226](#) for a definition of the Identify method. A SMASH-compliant management  
 579 service shall support the Identify method on each SMASH access port that it supports.

580 In addition to the child element defined in [DSP0226](#), the following extension elements are defined by  
 581 SMASH as children of the IdentifyResponse element:

```
582 <s:Body>
583   <wsmid:IdentifyResponse>
584     <wsmid:ProtocolVersion> xs:anyURI </wsmid:ProtocolVersion>
585     <wsmid:ProductVendor> xs:string </wsmid:ProductVendor>
586     <wsmid:ProductVersion> xs:string </wsmid:ProductVersion>
587     <SMASH:SMASHVersion> xs:string </SMASH:SMASHVersion>
588     <wsmid:SecurityProfiles>
589       <wsmid:SecurityProfileName> xs:string or URI </wsmid:SecurityProfileName> +
590     </wsmid:SecurityProfiles>
591   </wsmid:IdentifyResponse>
592 </s:Body>
```

593 Table 9 defines the IdentifyResponse payload requirements for SMASH 2.0.

594 **Table 9 – WS-Management IdentifyResponse Payload Elements**

Element	Requirement	Notes
wsmid:IdentifyResponse	Mandatory	The body of the response
wsmid:IdentifyResponse/wsmid:ProtocolVersion	Mandatory	URI identifying <a href="#">DSP0226</a> 1.0
wsmid:IdentifyResponse/wsmid:ProductVendor	Optional	
wsmid:IdentifyResponse/wsmid:ProductVersion	Optional	
wsmid:IdentifyResponse/SMASH:SMASHVersion	Mandatory	Identifies the SMASH version supported, which shall be formatted as “n.n.n” Example: “2.0.0”

Element	Requirement	Notes
wsmid:IdentifyResponse/wsmid:SecurityProfiles/ wsmid:SecurityProfileName	Mandatory	String identifying the security profile supported  <b>Class A:</b> "HTTP_DIGEST": <a href="http://schemas.dmtf.org/wbem/wsman/1/wsman/secprofile/http/digest">http://schemas.dmtf.org/wbem/wsman/1/wsman/secprofile/http/digest</a>  <b>Class B:</b> "HTTP_TLS_1": <a href="http://schemas.dmtf.org/wbem/wsman/1/wsman/secprofile/https/digest">http://schemas.dmtf.org/wbem/wsman/1/wsman/secprofile/https/digest</a> "HTTP_TLS_2": <a href="http://schemas.dmtf.org/wbem/wsman/1/wsman/secprofile/https/basic">http://schemas.dmtf.org/wbem/wsman/1/wsman/secprofile/https/basic</a> "HTTP_IPSEC": <a href="http://schemas.dmtf.org/wbem/wsman/1/wsman/secprofile/http/digest">http://schemas.dmtf.org/wbem/wsman/1/wsman/secprofile/http/digest</a>

## 595 8.2.2 wsmid:Identify Security Implementation Requirements

596 Implementations may support wsmid:Identify without authentication, as described in Rule R10.9-4 of  
 597 [DSP0226](#).

598 If an implementation supports wsmid:Identify without authentication, it should support it through a URL  
 599 that contains the suffix "/wsman-anon/identify."

600  
601  
602  
603

## **ANNEX A** (informative)

### **Change Log**

<b>Version</b>	<b>Date</b>	<b>Editor</b>	<b>Description</b>
1.0.0a	11/02/2006	A. Merkin	Preliminary Standard
2.0.0a	05/07/2007	J. Hilland	Preliminary Standard
2.0.0	05/15/2009	J. Hilland	DMTF Standard

604

## Bibliography

605 DMTF DSP2001, *Systems Management Architecture for Server Hardware (SMASH) Command Line*  
606 *Protocol (CLP) Architecture White Paper, 2.0,*  
607 [http://www.dmtf.org/standards/published\\_documents/DSP2001\\_2.0.pdf](http://www.dmtf.org/standards/published_documents/DSP2001_2.0.pdf)

608