



1  
2  
3  
4

**Document Number: DSP0232**

**Date: 2015-05-21**

**Version: 1.2.1**

## 5 **DASH Implementation Requirements**

6 **Supersedes: 1.2.0**  
7 **Document Class: Normative**  
8 **Document Status: Published**  
9 **Document Language: en-US**

10 Copyright Notice

11 Copyright © 2015 Distributed Management Task Force, Inc. (DMTF). All rights reserved.

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

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26 withdrawn or modified after publication, and shall be indemnified and held harmless by any party  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

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

32 This document's normative language is English. Translation into other languages is permitted.

33

# CONTENTS

34 Foreword ..... 5

35 Introduction..... 6

36 1 Scope ..... 7

37 2 Normative references ..... 7

38 2.1 Approved references..... 7

39 2.2 Other references ..... 9

40 3 Terms and definitions ..... 10

41 4 Symbols and abbreviated terms..... 11

42 5 Mandatory profiles and specifications ..... 11

43 6 Optional profiles ..... 13

44 7 Protocol implementation requirements..... 14

45 7.1 Management protocol ..... 14

46 7.2 Transport protocol..... 17

47 8 Security implementation requirements..... 17

48 8.1 Transport requirements..... 17

49 8.2 Roles and authorization ..... 18

50 8.3 User account management..... 19

51 8.4 Authentication mechanisms ..... 20

52 9 Discovery requirements..... 20

53 9.1 Network endpoint discovery stage..... 20

54 9.2 Management access point discovery stage..... 20

55 9.3 Enumeration of management capabilities stage..... 22

56 9.4 RegisteredSpecification instance..... 22

57 10 In-Band and Out-of-Band traffic requirements ..... 23

58 ANNEX A (informative) Change log ..... 24

59 Bibliography ..... 25

60

## 61 Tables

62 Table 1 – Mandatory profiles and specifications..... 12

63 Table 2 – Optional profiles ..... 13

64 Table 3 – WS-Transfer operations ..... 15

65 Table 4 – WS-Enumeration operations..... 15

66 Table 5 – WS-Eventing operations ..... 16

67 Table 6 – WS-Eventing Message security recommendations ..... 16

68 Table 7 – Required cryptographic algorithms or cipher suites..... 18

69 Table 8 – Operational roles supported by DASH..... 18

70 Table 9 – User account operations ..... 19

71 Table 10 – Authentication mechanisms ..... 20

72 Table 11 – WS-Management IdentifyResponse payload elements..... 21

73 Table 12 – CIM\_RegisteredSpecification element requirements..... 22

74



76

## Foreword

77 The *DASH Implementation Requirements* (DSP0232) was prepared by the Desktop and Mobile Working  
78 Group of the DMTF.

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

## 81 **Acknowledgments**

82 The authors wish to acknowledge the following people.

### 83 **Editors:**

- 84 • Hemal Shah – Broadcom Corporation
- 85 • Joe Kozlowski – Dell Inc.
- 86 • Steven Breed – Dell Inc.

### 87 **Contributors:**

- 88 • Stephen Fong – Advanced Micro Devices
- 89 • Bob Blair – Advanced Micro Devices
- 90 • Paul Vancil – Advanced Micro Devices
- 91 • Simon Assouad – Broadcom Corporation
- 92 • Murali Rajagopal – Broadcom Corporation
- 93 • Jon Hass – Dell Inc.
- 94 • Rick Landau – Dell Inc.
- 95 • Christoph Graham – Hewlett-Packard
- 96 • Jeff Hilland – Hewlett-Packard
- 97 • David Hines – Intel Corporation
- 98 • Joel Clark – Intel Corporation
- 99 • Andy Currid – NVIDIA Corporation
- 100 • Steve Hand – Symantec Corporation
- 101 • Jim Davis – WBEM Solutions

102

103

## Introduction

104 This specification describes the conformance requirements for implementing the Desktop and Mobile  
105 Architecture for System Hardware (DASH) version 1.2.

106

# DASH Implementation Requirements

## 107 1 Scope

108 This document describes the requirements for implementing the Desktop and Mobile Architecture for  
109 System Hardware version 1.2. This document does not define the implementation requirements directly.  
110 In clause 5, the mandatory profile specifications to be implemented are defined. In clause 6, the optional  
111 and conditional profile specifications are defined. Clauses 7, 8, 9, and 10 define the protocol, security,  
112 discovery, and management traffic requirements, respectively.

## 113 2 Normative references

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

### 117 2.1 Approved references

- 118 DMTF DSP0136, *Alert Standard Format Specification 2.0*,  
119 <http://www.dmtf.org/standards/documents/ASF/DSP0136.pdf>
- 120 DMTF DSP0200, *CIM Operations over HTTP 1.3*,  
121 [http://www.dmtf.org/standards/published\\_documents/DSP0200\\_1.3.pdf](http://www.dmtf.org/standards/published_documents/DSP0200_1.3.pdf)
- 122 DMTF DSP0226, *Web Services for Management 1.0*,  
123 [http://www.dmtf.org/standards/published\\_documents/DSP0226\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP0226_1.0.pdf)
- 124 DMTF DSP0227, *WS-Management CIM Binding Specification 1.0*,  
125 [http://www.dmtf.org/standards/published\\_documents/DSP0227\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP0227_1.0.pdf)
- 126 DMTF DSP0230, *WS-CIM Mapping Specification 1.0*,  
127 [http://www.dmtf.org/standards/published\\_documents/DSP0230\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP0230_1.0.pdf)
- 128 DMTF DSP1009, *Sensors Profile 1.0*,  
129 [http://www.dmtf.org/standards/published\\_documents/DSP1009\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP1009_1.0.pdf)
- 130 DMTF DSP1009, *Sensors Profile, 1.1*,  
131 [http://www.dmtf.org/standards/published\\_documents/DSP1009\\_1.1.pdf](http://www.dmtf.org/standards/published_documents/DSP1009_1.1.pdf)
- 132 DMTF DSP1010, *Record Log Profile, 2.0*,  
133 [http://www.dmtf.org/standards/published\\_documents/DSP1010\\_2.0.pdf](http://www.dmtf.org/standards/published_documents/DSP1010_2.0.pdf)
- 134 DMTF DSP1011, *Physical Asset Profile 1.0*,  
135 [http://www.dmtf.org/standards/published\\_documents/DSP1011\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP1011_1.0.pdf)
- 136 DMTF DSP1012, *Boot Control Profile 1.0*,  
137 [http://www.dmtf.org/standards/published\\_documents/DSP1012\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP1012_1.0.pdf)
- 138 DMTF DSP1013, *Fan Profile 1.0*,  
139 [http://www.dmtf.org/standards/published\\_documents/DSP1013\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP1013_1.0.pdf)
- 140 DMTF DSP1014, *Ethernet Port Profile, 1.0*,  
141 [http://www.dmtf.org/standards/published\\_documents/DSP1014\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP1014_1.0.pdf)

- 142 DMTF DSP1015, *Power Supply Profile 1.0*,  
143 [http://www.dmtf.org/standards/published\\_documents/DSP1015\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP1015_1.0.pdf)
- 144 DMTF DSP1015, *Power Supply Profile, 1.1*,  
145 [http://www.dmtf.org/standards/published\\_documents/DSP1015\\_1.1.pdf](http://www.dmtf.org/standards/published_documents/DSP1015_1.1.pdf)
- 146 DMTF DSP1016, *Telnet Service Profile, 1.0*,  
147 [http://www.dmtf.org/standards/published\\_documents/DSP1016\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP1016_1.0.pdf)
- 148 DMTF DSP1017, *SSH Service Profile, 1.0*,  
149 [http://www.dmtf.org/standards/published\\_documents/DSP1017\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP1017_1.0.pdf)
- 150 DMTF DSP1018, *Service Processor Profile, 1.1*,  
151 [http://www.dmtf.org/standards/published\\_documents/DSP1018\\_1.1.pdf](http://www.dmtf.org/standards/published_documents/DSP1018_1.1.pdf)
- 152 DMTF DSP1022, *CPU Profile 1.0*,  
153 [http://www.dmtf.org/standards/published\\_documents/DSP1022\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP1022_1.0.pdf)
- 154 DMTF DSP1023, *Software Inventory Profile 1.0*,  
155 [http://www.dmtf.org/standards/published\\_documents/DSP1023\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP1023_1.0.pdf)
- 156 DMTF DSP1024, *Text Console Redirection Profile 1.0*,  
157 [http://www.dmtf.org/standards/published\\_documents/DSP1024\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP1024_1.0.pdf)
- 158 DMTF DSP1025, *Software Update Profile 1.0*,  
159 [http://www.dmtf.org/standards/published\\_documents/DSP1025\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP1025_1.0.pdf)
- 160 DMTF DSP1026, *System Memory Profile 1.0*,  
161 [http://www.dmtf.org/standards/published\\_documents/DSP1026\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP1026_1.0.pdf)
- 162 DMTF DSP1027, *Power State Management Profile 1.0*,  
163 [http://www.dmtf.org/standards/published\\_documents/DSP1027\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP1027_1.0.pdf)
- 164 DMTF DSP1027, *Power State Management Profile 2.0*,  
165 [http://www.dmtf.org/standards/published\\_documents/DSP1027\\_2.0.pdf](http://www.dmtf.org/standards/published_documents/DSP1027_2.0.pdf)
- 166 DMTF DSP1029, *OS Status Profile 1.0*,  
167 [http://www.dmtf.org/standards/published\\_documents/DSP1029\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP1029_1.0.pdf)
- 168 DMTF DSP1029, *OS Status Profile, 1.1*,  
169 [http://www.dmtf.org/standards/published\\_documents/DSP1029\\_1.1.pdf](http://www.dmtf.org/standards/published_documents/DSP1029_1.1.pdf)
- 170 DMTF DSP1030, *Battery Profile 1.0*,  
171 [http://www.dmtf.org/standards/published\\_documents/DSP1030\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP1030_1.0.pdf)
- 172 DMTF DSP1033, *Profile Registration Profile 1.0*,  
173 [http://www.dmtf.org/standards/published\\_documents/DSP1033\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP1033_1.0.pdf)
- 174 DMTF DSP1034, *Simple Identity Management Profile 1.0*,  
175 [http://www.dmtf.org/standards/published\\_documents/DSP1034\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP1034_1.0.pdf)
- 176 DMTF DSP1035, *Host LAN Network Port Profile 1.0*,  
177 [http://www.dmtf.org/standards/published\\_documents/DSP1035\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP1035_1.0.pdf)
- 178 DMTF DSP1036, *IP Interface Profile 1.0*,  
179 [http://www.dmtf.org/standards/published\\_documents/DSP1036\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP1036_1.0.pdf)
- 180 DMTF DSP1037, *DHCP Client Profile 1.0*,  
181 [http://www.dmtf.org/standards/published\\_documents/DSP1037\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP1037_1.0.pdf)
- 182 DMTF DSP1038, *DNS Client Profile 1.0*,  
183 [http://www.dmtf.org/standards/published\\_documents/DSP1038\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP1038_1.0.pdf)



- 184 DMTF DSP1039, *Role Based Authorization Profile 1.0*,  
185 [http://www.dmtf.org/standards/published\\_documents/DSP1039\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP1039_1.0.pdf)
- 186 DMTF DSP1040, *Watchdog Profile, 1.0*,  
187 [http://www.dmtf.org/standards/published\\_documents/DSP1040\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP1040_1.0.pdf)
- 188 DMTF DSP1054, *Indications Profile 1.0*,  
189 [http://www.dmtf.org/standards/published\\_documents/DSP1054\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP1054_1.0.pdf)
- 190 DMTF DSP1058, *Base Desktop and Mobile Profile 1.0*,  
191 [http://www.dmtf.org/standards/published\\_documents/DSP1058\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP1058_1.0.pdf)
- 192 DMTF DSP1061, *BIOS Management Profile 1.0*,  
193 [http://www.dmtf.org/standards/published\\_documents/DSP1061\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP1061_1.0.pdf)
- 194 DMTF DSP1070, *Opaque Management Data Profile 1.0*,  
195 [http://www.dmtf.org/standards/published\\_documents/DSP1070\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP1070_1.0.pdf)
- 196 DMTF DSP1074, *Indicator LED Profile, 1.0*,  
197 [http://www.dmtf.org/standards/published\\_documents/DSP1074\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP1074_1.0.pdf)
- 198 DMTF DSP1075, *PCI Device Profile, 1.0*,  
199 [http://www.dmtf.org/standards/published\\_documents/DSP1075\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP1075_1.0.pdf)
- 200 DMTF DSP1076, *KVM Redirection 1.0*,  
201 [http://www.dmtf.org/standards/published\\_documents/DSP1076\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP1076_1.0.pdf)
- 202 DMTF DSP1077, *USB Redirection Profile 1.0*,  
203 [http://www.dmtf.org/standards/published\\_documents/DSP1077\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP1077_1.0.pdf)
- 204 DMTF DSP1086, *Media Redirection Profile 1.0*,  
205 [http://www.dmtf.org/standards/published\\_documents/DSP1086\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP1086_1.0.pdf)
- 206 DMTF DSP1108, *Physical Computer System View Profile, 1.0*,  
207 [http://www.dmtf.org/standards/published\\_documents/DSP1108\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP1108_1.0.pdf)
- 208 DMTF DSP1116, *IP Configuration Profile, 1.0*,  
209 [http://www.dmtf.org/standards/published\\_documents/DSP1116\\_1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP1116_1.0.pdf)
- 210 DMTF DSP8007 *Platform Message Registry 1.0*,  
211 [http://schemas.dmtf.org/wbem/messageregistry/1/dsp8007\\_1.0.xml](http://schemas.dmtf.org/wbem/messageregistry/1/dsp8007_1.0.xml)
- 212 DMTF DSP8030, *DASH Namespace Schema 1.0*, <http://schemas.dmtf.org/wbem/dash/1/dash.xsd>
- 213 IETF RFC 2246, T. Dierks et al., *The TLS Protocol Version 1.0*, <http://www.ietf.org/rfc/rfc2246.txt>
- 214 IETF RFC 4106, J. Viega and D. McGrew, *The Use of Galois/Counter Mode (GCM) in IPsec*  
215 *Encapsulating Security Payload (ESP)*, <http://www.rfc-editor.org/rfc/rfc4106.txt>
- 216 IETF RFC 4301, S. Kent, *Security Architecture for the Internet Protocol*,  
217 <http://www.rfc-editor.org/rfc/rfc4301.txt>
- 218 IETF RFC 4303, S. Kent, *IP Encapsulating Security Payload*, <http://www.ietf.org/rfc/rfc4303.txt>
- 219 IETF RFC 4346, T. Dierks et al., *The TLS Protocol Version 1.1*, <http://www.ietf.org/rfc/rfc4346.txt>
- 220 IETF RFC 5246, T. Dierks et al., *The TLS Protocol Version 1.2*, <http://www.ietf.org/rfc/rfc5246.txt>

## 2.2 Other references

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

## 224 3 Terms and definitions

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

226 3.1

227 **can**

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

229 3.2

230 **cannot**

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

232 3.3

233 **conditional**

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

236 3.4

237 **mandatory**

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

240 3.5

241 **may**

242 indicates a course of action permissible within the limits of the document

243 3.6

244 **need not**

245 indicates a course of action permissible within the limits of the document

246 3.7

247 **optional**

248 indicates a course of action permissible within the limits of the document

249 3.8

250 **shall**

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

253 3.9

254 **shall not**

255 indicates requirements to be followed in order to conform to the document and from which no deviation is  
256 permitted

257 3.10

258 **should**

259 indicates that among several possibilities, one is recommended as particularly suitable, without  
260 mentioning or excluding others, or that a certain course of action is preferred but not necessarily required

261 3.11

262 **should not**

263 indicates that a certain possibility or course of action is deprecated but not prohibited

## 264 **4 Symbols and abbreviated terms**

265 The following symbols and abbreviations are used in this document.

### 266 **4.1**

#### 267 **ASF**

268 Alert Standard Format

### 269 **4.2**

#### 270 **IANA**

271 Internet Assigned Numbers Authority

### 272 **4.3**

#### 273 **IP**

274 Internet Protocol

### 275 **4.4**

#### 276 **MAC**

277 Media Access Control

### 278 **4.5**

#### 279 **MAP**

280 Management Access Point

### 281 **4.6**

#### 282 **RMCP**

283 Remote Management and Control Protocol

### 284 **4.7**

#### 285 **TCP**

286 Transmission Control Protocol

### 287 **4.8**

#### 288 **TLS**

289 Transport Layer Security

### 290 **4.9**

#### 291 **UDP**

292 User Datagram Protocol

### 293 **4.10**

#### 294 **URI**

295 Uniform Resource Identifier

### 296 **4.11**

#### 297 **WS**

298 Web Services

## 299 **5 Mandatory profiles and specifications**

300 The mandatory profiles and specifications shown in Table 1 shall be implemented in accordance with this  
301 specification.

302

Table 1 – Mandatory profiles and specifications

Name	Number	Version	Description
<i>Base Desktop and Mobile Profile</i>	<a href="#">DSP1058</a>	1.0	
<i>Profile Registration Profile</i>	<a href="#">DSP1033</a>	1.0	
<i>Role Based Authorization Profile</i>	<a href="#">DSP1039</a>	1.0	
<i>Simple Identity Management Profile</i>	<a href="#">DSP1034</a>	1.0	
<i>WS-Management Specification</i>	<a href="#">DSP0226</a>	1.0	
<i>WS-Management CIM Binding Specification</i>	<a href="#">DSP0227</a>	1.0	
<i>WS-CIM Mapping Specification</i>	<a href="#">DSP0230</a>	1.0	

303 **6 Optional profiles**

304 The optional profiles shown in Table 2 may be implemented. When a profile in Table 2 is implemented,  
 305 the requirements specified in this section shall be met. For an optional profile with multiple versions listed  
 306 in the table below, one or more versions of the optional profile may be implemented. If implemented, the  
 307 latest version of the listed optional profile should be implemented.

308 **Table 2 – Optional profiles**

Name	Number	Version	Description
Battery Profile	<a href="#">DSP1030</a>	1.0	
BIOS Management Profile	<a href="#">DSP1061</a>	1.0	
Boot Control Profile	<a href="#">DSP1012</a>	1.0	
CPU Profile	<a href="#">DSP1022</a>	1.0	
DHCP Client Profile	<a href="#">DSP1037</a>	1.0	
DNS Client Profile	<a href="#">DSP1038</a>	1.0	
Ethernet Port Profile	<a href="#">DSP1014</a>	1.0	
Fan Profile	<a href="#">DSP1013</a>	1.0	
Host LAN Network Port Profile	<a href="#">DSP1035</a>	1.0	
Indications Profile	<a href="#">DSP1054</a>	1.0	An instance of one of the concrete subclasses of CIM_Indication shall be the payload of a WS-Eventing message. The contents for AlertIndication should be drawn from <i>Platform Message Registry</i> ( <a href="#">DSP8007</a> ).  It is recommended that any vendor-specific messages are formulated with a published message registry with the owning entity other than the DMTF. Vendor-specific messages should be defined in a vendor-specific message registry that is conformant with the DMTF Message Registry Schema, as defined in <a href="#">DSP4006</a> .
Indicator LED Profile	<a href="#">DSP1074</a>	1.0	
IP Interface Profile	<a href="#">DSP1036</a>	1.0	
IP Configuration Profile	<a href="#">DSP1116</a>	1.0	
KVM Redirection Profile	<a href="#">DSP1076</a>	1.0	
Media Redirection Profile	<a href="#">DSP1086</a>	1.0	
Opaque Management Data Profile	<a href="#">DSP1070</a>	1.0	
OS Status Profile	<a href="#">DSP1029</a>	1.0	
OS Status Profile	<a href="#">DSP1029</a>	1.1	
PCI Device Profile	<a href="#">DSP1075</a>	1.0	
Physical Asset Profile	<a href="#">DSP1011</a>	1.0	
Physical Computer System View Profile	<a href="#">DSP1108</a>	1.0	
Power State Management Profile	<a href="#">DSP1027</a>	1.0	
Power State Management Profile	<a href="#">DSP1027</a>	2.0	
Power Supply Profile	<a href="#">DSP1015</a>	1.0	
Power Supply Profile	<a href="#">DSP1015</a>	1.1	
Record Log Profile	<a href="#">DSP1010</a>	2.0	

Name	Number	Version	Description
<i>Sensors Profile</i>	<a href="#">DSP1009</a>	1.0	
<i>Sensors Profile</i>	<a href="#">DSP1009</a>	1.1	
<i>Service Processor Profile</i>	<a href="#">DSP1018</a>	1.1	
<i>Software Inventory Profile</i>	<a href="#">DSP1023</a>	1.0	
<i>Software Update Profile</i>	<a href="#">DSP1025</a>	1.0	
<i>SSH Service Profile</i>	<a href="#">DSP1017</a>	1.0	
<i>System Memory Profile</i>	<a href="#">DSP1026</a>	1.0	
<i>Telnet Service Profile</i>	<a href="#">DSP1016</a>	1.0	
<i>Text Console Redirection Profile</i>	<a href="#">DSP1024</a>	1.0	
<i>USB Redirection Profile</i>	<a href="#">DSP1077</a>	1.0	
<i>Watchdog Profile</i>	<a href="#">DSP1040</a>	1.0	

## 309 7 Protocol implementation requirements

310 A DASH-compliant implementation shall use a CIM-based data model for representing managed  
 311 resources and services. This section describes the Management Protocol and Transport Protocol  
 312 requirements for a DASH implementation.

### 313 7.1 Management protocol

314 It is mandatory for DASH implementations to use the protocol defined in *Web Services for Management*  
 315 *Specification* ([DSP0226](#)) as the management protocol for supporting operations. The implementation of  
 316 the Web Services Management protocol shall expose CIM schema.

#### 317 7.1.1 XML namespaces

318 The following URI identifies an XML namespace that contains DASH-specific XML definitions

319 (1) <http://schemas.dmtf.org/wbem/dash/1/dash.xsd>

#### 320 7.1.2 WS-Transfer

321 It is mandatory for DASH implementations to support WS-Transfer as described in clause 7 of [DSP0226](#).  
 322 Table 3 defines support for WS-Transfer operations and their respective DASH requirements.

323

**Table 3 – WS-Transfer operations**

Operation	Requirement	Notes
Get	Mandatory	This operation retrieves resource representations.
Put	Conditional	This operation updates resources. If an implemented profile requires ModifyInstance support, the Put operation shall be supported to fulfill that requirement.
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.

324 **7.1.3 WS-Enumeration**

325 It is mandatory for DASH implementations to support WS-Enumeration as described in clause 8 of  
 326 [DSP0226](#). Table 4 defines support for WS-Enumeration operations and their respective DASH  
 327 requirements.

328

**Table 4 – 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 R8.1-4 in <a href="#">DSP0226</a> . Implementation of this operation is not recommended.
GetStatus	Optional	See Rule R8.1-4 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 R8.1-4 in <a href="#">DSP0226</a> . Implementation of this operation is not recommended.

329 It is recommended that the wsman:OptimizeEnumeration option be implemented as a child element of the  
 330 wsen:Enumerate element. Refer to clause 8.2.3 of [DSP0226](#) for details. The service shall accept the  
 331 element, but it does not have to honor it as described in Rule R8.2.3-1 of [DSP0226](#).

332 **7.1.3.1 WS-Enumeration filter dialects**

333 It is optional for DASH implementations to support Selector Filter Dialect for filtered enumeration and  
 334 subscription as described in Annex E of [DSP0226](#). This recommendation does not contravene Rule  
 335 R8.2.1-5 of [DSP0226](#).

336 It is optional for DASH implementations to support *Association Queries* with the dialect filter URI as  
 337 specified in [DSP0227](#).

338 It is optional for DASH implementations to support the CQL filter dialect for enumeration as described in  
 339 clause 7.1 of [DSP0227](#). This clause does not contravene Rule R8.2.1-5 of [DSP0226](#).

#### 340 7.1.4 WS-Eventing

341 Support for WS-Eventing is conditional. A service advertising conformance to the *Indications Profile* shall  
 342 support WS-Eventing as described in clause 10 of [DSP0226](#) and is further constrained by the definition  
 343 described in this section 7.1.4. Table 5 defines support for WS-Eventing operations and their respective  
 344 DASH requirements.

345 **Table 5 – WS-Eventing operations**

Operation	Requirement	Notes
Subscribe	Mandatory	
Renew	Mandatory	
Unsubscribe	Mandatory	
SubscriptionEnd	Optional	
GetStatus	Optional	See Rule R10.3-1 in <a href="#">DSP0226</a> . Implementation of this operation is not recommended.

##### 346 7.1.4.1 WS-Eventing messaging security

347 For WS-Eventing the messaging security defined in Table 6 should be followed.

348 **Table 6 – 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 8.1, because it can carry sensitive information	Subscriber
	wse:Renew	Class B, because it can carry sensitive information	Subscriber
	wse:SubscriptionEnd	Class B, because it can carry sensitive information	Subscriber
	wse:Unsubscribe	Class B, because it can carry sensitive information	Subscriber
Delivery	wse:Delivery (Push)	Class A or B as defined in section 8.1 (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 (B for sensitive information)	MAP, but not necessarily with its own credentials
	wse:Delivery (Batched)	Class A or B (B for sensitive information)	MAP, but not necessarily with its own credentials
	wsen:Pull (Pull delivery)	Class A or B (B for sensitive information)	Subscriber



#### 349 7.1.4.2 WS-Eventing delivery mode

350 DASH implementations shall support WS-Eventing Push Mode as described in clause 10.2.9.2 of  
351 [DSP0226](#). DASH implementations should support WS-Eventing PushWithAck Mode as described in  
352 clause 10.2.9.3 of [DSP0226](#).

#### 353 7.1.4.3 Subscription related property definition guidance

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

356 The value for the FailureTriggerTimeInterval property on the CIM\_IndicationSubscription or  
357 CIM\_FilterCollectionSubscription instance created internally in response to wse:Subscribe should be to  
358 30 seconds.

### 359 7.2 Transport protocol

360 DASH implementations shall use HTTP 1.1 as the SOAP transport for [DSP0226](#). For detailed information  
361 about the transport protocol required by DASH, refer to section 5.2 of the *Systems Management*  
362 *Architecture for Mobile and Desktop Hardware White Paper* ([DSP2014](#)).

## 363 8 Security implementation requirements

364 This section describes transport requirements, roles and authorization, user account management, and  
365 authentication.

### 366 8.1 Transport requirements

367 DASH defines two security classes for HTTP 1.1 transport:

368 1) **Class A:** The security class A requires HTTP digest authentication for the user authentication.  
369 For this class, no encryption capabilities are required beyond the encryption of the password  
370 during the digest authentication exchange. If class A is implemented, MD5 digest algorithm shall  
371 be supported.

372 • **String = "HTTP\_DIGEST"**

373 – URI = <http://schemas.dmtf.org/wbem/wsman/1/wsman/secprofile/http/digest>

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

377 • **String = "HTTP\_TLS\_1"**

378 – URI = <http://schemas.dmtf.org/wbem/wsman/1/wsman/secprofile/https/digest>

379 • **String = "HTTP\_TLS\_2"**

380 – URI = <http://schemas.dmtf.org/wbem/wsman/1/wsman/secprofile/https/basic>

381 • **String = "HTTP\_IPSEC"**

382 – URI = <http://schemas.dmtf.org/wbem/wsman/1/wsman/secprofile/http/digest/ipsec>

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

385 Refer to 7.1.4.1 for WS-Eventing security requirements.

386 **8.1.1 Cryptographic algorithms and cipher suites**387 Table 7 lists the required cryptographic algorithms or cipher suites for the security profiles mentioned in  
388 this section.389 **Table 7 – Required cryptographic algorithms or cipher suites**

Security Profile	Required Algorithm(s) or Cipher suite	Notes
"HTTP_DIGEST"	MD5	
"HTTP_TLS_1"	TLS_RSA_WITH_AES_128_CBC_SHA (for TLS) and MD5 (for HTTP digest)	TLS version 1.0 or later  Refer to RFC 2246, RFC 4346, RFC 5246 and RFC 3268.  It is recommended that the latest 1.x version of TLS is implemented.
"HTTP_TLS_2"	TLS_RSA_WITH_AES_128_CBC_SHA	TLS version 1.0 or later  Refer to RFC 2246, RFC 4346, RFC 5246 and RFC 3268.  It is recommended that the latest 1.x version of TLS is implemented.
"HTTP_IPSEC"	For IPsec: AES-GCM (key size: 128 bits, ICV or Digest len: 16 B) or AES-CBC (Key size: 128 bits) with HMAC-SHA1-96 and  For HTTP digest: MD5	Refer to RFC <a href="#">4301</a> , <a href="#">4303</a> , and <a href="#">4106</a>

390 **8.2 Roles and authorization**391 Table 8 outlines the Operational Roles supported by DASH implementations and the respective DASH  
392 requirements.393 **Table 8 – Operational roles supported by DASH**

Operational Role	Requirement	Notes
Read-only User	Optional	For detailed description of these roles see <a href="#">DSP2014</a> .
Operator	Optional	
Administrator	Mandatory	

394 A DASH-compliant service shall support the administrator role. An implementation may support the  
395 operator and/or read-only user roles. All roles shall be modeled using [DSP1039](#), *Role Based*  
396 *Authorization Profile, 1.0*.

397 **8.3 User account management**

398 The authentication and authorization mechanisms defined are tied with user account management. DASH  
 399 implementations shall support a role-based authorization model.

400 Each user shall have the ability to modify its own account credentials, depending on the user’s privileges.  
 401 An account in the administrator role shall be able to perform account management for all users. Table 9  
 402 outlines the operations supported for user account management and the respective DASH requirements.

403 **Table 9 – 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	Mandatory	Required for the administrator account.
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

404 The modifications of privileges include the changing of bindings between accounts or groups and roles.  
 405 All operations defined in Table 9 shall be performed using operations as defined in DMTF [DSP1039](#), *Role*  
 406 *Based Authorization Profile, 1.0* and DMTF [DSP1034](#), *Simple Identity Management Profile, 1.0*.

## 407 8.4 Authentication mechanisms

408 DASH implementations shall support User-Level authentication. DASH implementations may support two-  
409 level (Machine-Level and User-Level) authentication.

410 Table 10 outlines requirements for the three types of authentication mechanisms supported by DASH 1.0  
411 implementations.

412 **Table 10 – Authentication mechanisms**

Authentication Mechanisms	Requirement	Notes
Machine-Level	Optional	
User-Level	Mandatory	
Third-Party	Optional	

## 413 9 Discovery requirements

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

### 417 9.1 Network endpoint discovery stage

418 Section 8.2 of the *Systems Management Architecture for Mobile and Desktop Hardware White Paper*  
419 ([DSP2014](#)) describes endpoint discovery methods. A DASH 1.1 compliant implementation need not  
420 support any of the described methods.

### 421 9.2 Management access point discovery stage

422 A DASH-compliant MAP should support the following phase process for MAP discovery:

- 423 • **Phase 1:** RMCP Presence Ping/Pong.

424 A DASH-compliant MAP shall support the following phase process for MAP discovery:

- 425 • **Phase 2:** WS-Management Identify method.

#### 426 9.2.1 RMCP Presence Ping/Pong

427 Presence Ping is an RMCP command that is defined in the *Alert Standard Format Specification*,  
428 ([DSP0136](#)). The command involves a request-response message exchange initiated by a management  
429 client (Ping) and completed by a management service (Pong).

430 The format of the RMCP Presence Pong (40h) data section shall conform to section 3.2.4.3 of [DSP0136](#)  
431 with the following definition:  
432

433 *Supported Interactions* field (Data Byte 10 of Presence Pong), bit 5 set to 1b if DASH is supported

434 A DASH-compliant MAP should support this command on the ASF-RMCP well-known UDP port (623)  
435 and/or well-known UDP port (664).

436 **9.2.2 WS-Management Identify method**

437 Refer to clause 11 of [DSP0226](#) for a definition of the Identify method. A DASH-compliant management  
 438 service shall support the Identify method on each TCP port on which WS-Management service is  
 439 supported.

440 In addition to the child element defined in [DSP0226](#), the following extension elements are defined by  
 441 DASH as children of the *IdentifyResponse* element:

```

442 <s:Body>
443   <wsmid:IdentifyResponse>
444     <wsmid:ProtocolVersion> xs:anyURI </wsmid:ProtocolVersion>
445     <wsmid:ProductVendor> xs:string </wsmid:ProductVendor>
446     <wsmid:ProductVersion> xs:string </wsmid:ProductVersion>
447     <dash:DASHVersion> xs:string </dash:DASHVersion>
448     <wsmid:SecurityProfiles>
449       <wsmid:SecurityProfileName> xs:string or URI </wsmid:SecurityProfileName> +
450     </wsmid:SecurityProfiles>
451   </wsmid:IdentifyResponse>
452 </s:Body>
    
```

453 Table 11 defines the IdentifyResponse payload requirements for DASH 1.1.

454 **Table 11 – 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 http://schemas.dmtf.org/wbem/wsman/1/wsman.xsd
wsmid:IdentifyResponse/wsmid:ProductVendor	Optional	
wsmid:IdentifyResponse/wsmid:ProductVersion	Optional	
wsmid:IdentifyResponse/dash:DASHVersion	Mandatory	Identifies the version of the <i>DASH Implementation Requirements</i> specification that is supported, which shall be in the form “M.N.U”, where M represents major version, N represents minor version, and U represents update version of the specification. For this specification, the value shall be set to “1.1.0”.

Element	Requirement	Notes
wsmid:IdentifyResponse/wsmid:SecurityProfiles/ wsmid:SecurityProfileName	Mandatory	URI 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>

455 **9.2.3 wsmid:Identify security implementation requirements**

456 Implementations may support wsmid:Identify without authentication as described in Rule R11.4 of  
 457 [DSP0226](#).

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

460 **9.3 Enumeration of management capabilities stage**

461 The DMTF *Profile Registration Profile* ([DSP1033](#)) specifies methods for enumerating the management  
 462 capabilities of a CIM-based management access point in a scalable manner. Scalability here refers to the  
 463 fact that each registered profile concisely describes support for a set of related management capabilities  
 464 that is independent of the number of CIM instances supported by the management access point.

465 **9.4 RegisteredSpecification instance**

466 The DASH implementation should support an instance of CIM\_RegisteredSpecification to indicate  
 467 support for this version of the specification.

468 Table 12 identifies the element requirements for CIM\_RegisteredSpecification.

469 **Table 12 – CIM\_RegisteredSpecification element requirements**

Element	Requirement	Description
<b>Properties</b>		
InstanceID	Mandatory	Key, see schema definition.
SpecificationType	Mandatory	This property shall have a value of 3 ("Initiative Wrapper").
RegisteredOrganization	Mandatory	This property shall have a value of 2 (DMTF).
RegisteredName	Mandatory	This property shall have a value of "DASH".
RegisteredVersion	Mandatory	This property shall have a value of "1.2.1".

Element	Requirement	Description
AdvertiseTypes	Mandatory	Required, see Schema definition.
AdvertiseTypeDescriptions	Mandatory	See Schema definition.
<b>Operations</b>		
GetInstance	Mandatory	
EnumerateInstances	Mandatory	
EnumerateInstanceNames	Mandatory	

470 The instance of CIM\_RegisteredSpecification shall be exposed in the interop namespace. The instance to  
 471 CIM\_RegisteredSpecification shall be associated with at least one instance of CIM\_RegisteredProfile of  
 472 one of the mandatory profiles defined in this specification using an instance of  
 473 CIM\_ReferencedSpecification. The Antecedent property of the instance of CIM\_ReferencedSpecification  
 474 shall reference the instance of the CIM\_RegisteredProfile. The Dependent property of the instance of  
 475 CIM\_ReferencedSpecification shall reference the instance CIM\_RegisteredSpecification.

476 **10 In-Band and Out-of-Band traffic requirements**

477 A DASH compliant service shall support, at minimum, a shared IPv4 and MAC address as defined below:

- 478 • A physical system’s out-of-band Management Access Point and the In-Band host shall share  
 479 the MAC address and IPv4 address of the network interface. Manageability traffic shall be  
 480 routed to the MAP through the well-known system ports defined by IANA. Implementations may  
 481 support the use and configuration of other ports.

482 Developers may use any port necessary during product development. Implementations shall support the  
 483 IANA-defined system ports for product deployment.

- 484 • Sideband: TCP ports for WS-Management Service
  - 485 – OOB-WS-HTTP
  - 486 – TCP 623
  - 487 – OOB-WS-HTTPS
  - 488 – TCP 664 (If class B is implemented)
- 489 • In-band: TCP ports for WS-Management Service may be supported on the following transport  
 490 ports and shall be transport specific:
  - 491 – HTTP
  - 492 – HTTPS (If class B is implemented)

493 NOTE: In-band and out-of-band MAPs shall listen on different ports.

494  
495  
496  
497  
498

## ANNEX A (informative)

### Change log

Version	Date	Description
1.0.0	2009-05-19	
1.1.0	2009-06-22	DMTF Standard Release
1.2.0	2014-10-19	DMTF Standard Release
1.2.1	2015-05-21	Resolves Mantis #2253.



499

## Bibliography

500

501 DMTF DSP2014, *Systems Management Architecture for Mobile and Desktop Hardware White Paper*  
502 *1.1.0*, [http://www.dmtf.org/standards/published\\_documents/DSP2014\\_1.1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP2014_1.1.0.pdf)  
503 (Informative text in this document details Protocol, Security, and Discovery.)

504 DMTF DSP4006, *Standard Registry Development and Publication Process 1.1*,  
505 [http://www.dmtf.org/standards/published\\_documents/DSP4006\\_1.1.0.pdf](http://www.dmtf.org/standards/published_documents/DSP4006_1.1.0.pdf)

506