



Document Number: DSP0232

Date: 2022-01-01

Version: 1.3.1

DASH Implementation Requirements

Supersedes: 1.3.0

Document Class: Normative

Document Status: Published

Document Language: en-US

Copyright Notice

Copyright © 2009, 2014-2015, 2021, 2022 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patent owner or claimant, and shall have no liability or responsibility for costs or losses incurred if a standard is withdrawn or modified after publication, and shall be indemnified and held harmless by any party implementing the standard from any and all claims of infringement by a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>.

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

CONTENTS

Foreword 4

Introduction 5

1 Scope 6

2 Normative references 6

3 Terms and definitions 9

4 Symbols and abbreviated terms 10

5 Mandatory profiles and specifications 11

6 Optional profiles 12

7 Protocol implementation requirements 13

 7.1 Management protocol 13

 7.2 Transport protocol 16

8 Security implementation requirements 16

 8.1 Transport requirements 16

 8.2 Roles and authorization 18

 8.3 User account management 18

 8.4 Authentication mechanisms 19

9 Discovery requirements 19

 9.1 Network endpoint discovery stage 19

 9.2 Management access point discovery stage 19

 9.3 Enumeration of management capabilities stage 21

 9.4 RegisteredSpecification instance 21

10 In-band and out-of-band traffic requirements 22

ANNEX A (informative) Change log 23

Bibliography 24

Tables

Table 1 – Mandatory profiles and specifications 11

Table 2 – Optional profiles 12

Table 3 – WS-Transfer operations 14

Table 4 – WS-Enumeration operations 14

Table 5 – WS-Eventing operations 15

Table 6 – WS-Eventing message security recommendations 15

Table 7 – Required cryptographic algorithms or cipher suites 17

Table 8 – Operational Roles Supported by DASH 18

Table 9 – User account operations 18

Table 10 – Authentication mechanisms 19

Table 11 – WS-Management IdentifyResponse payload elements 20

Table 12 – CIM_RegisteredSpecification element requirements 22

Foreword

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

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

Acknowledgments

The DMTF acknowledges the following individuals for their contributions to this document:

Editors:

- Hemal Shah – Broadcom Inc.
- Joe Kozlowski – Dell Inc.
- Steven Breed – Dell Inc.

Contributors:

- Simon Assouad – Broadcom Corporation
- Bob Blair – Advanced Micro Devices
- Joel Clark – Intel Corporation
- Andy Currid – NVIDIA Corporation
- Jim Davis – WBEM Solutions
- Stephen Fong – Advanced Micro Devices
- Christoph Graham – Hewlett-Packard
- Steve Hand – Symantec Corporation
- Jon Hass – Dell Inc.
- Jeff Hilland – Hewlett-Packard
- David Hines – Intel Corporation
- Rick Landau – Dell Inc.
- Divyanand Malavalli - Advanced Micro Devices
- Murali Rajagopal – Broadcom Corporation
- Siva Sathappan - Advanced Micro Devices
- Paul Vancil – Advanced Micro Devices

Introduction

This specification describes the conformance requirements for implementing the Desktop and Mobile Architecture for System Hardware (DASH) version 1.3.

1

DASH Implementation Requirements

1 Scope

3 This document describes the requirements for implementing the Desktop and Mobile Architecture for
4 System Hardware version 1.3. This document does not define the implementation requirements directly.
5 In clause 5, the mandatory profile specifications to be implemented are defined. In clause 6, the optional
6 and conditional profile specifications are defined. Clauses 7, 8, 9, and 10 define the protocol, security,
7 discovery, and management traffic requirements, respectively.

2 Normative references

9 The following referenced documents are indispensable for the application of this document. For dated or
10 versioned references, only the edition cited (including any corrigenda or DMTF update versions) applies.
11 For references without a date or version, the latest published edition of the referenced document
12 (including any corrigenda or DMTF update versions) applies.

13 DMTF DSP0136, *Alert Standard Format Specification 2.0*,
14 <https://www.dmtf.org/sites/default/files/standards/documents/DSP0136.pdf>

15 DMTF DSP0200, *CIM Operations over HTTP 1.3*,
16 https://www.dmtf.org/sites/default/files/standards/documents/DSP0200_1.3.pdf

17 DMTF DSP0226, *Web Services for Management 1.0*,
18 http://www.dmtf.org/standards/published_documents/DSP0226_1.0.pdf

19 DMTF DSP0227, *WS-Management CIM Binding Specification 1.0*,
20 https://www.dmtf.org/sites/default/files/standards/documents/DSP0227_1.0.pdf

21 DMTF DSP0230, *WS-CIM Mapping Specification 1.0*,
22 http://www.dmtf.org/standards/published_documents/DSP0230_1.0.pdf

23 DMTF DSP1009, *Sensors Profile 1.0*,
24 https://www.dmtf.org/sites/default/files/standards/documents/DSP1009_1.0.pdf

25 DMTF DSP1009, *Sensors Profile, 1.1*,
26 http://www.dmtf.org/standards/published_documents/DSP1009_1.1.pdf

27 DMTF DSP1010, *Record Log Profile, 2.0*,
28 https://www.dmtf.org/sites/default/files/standards/documents/DSP1010_2.0.pdf

29 DMTF DSP1011, *Physical Asset Profile 1.0*,
30 http://www.dmtf.org/standards/published_documents/DSP1011_1.0.pdf

31 DMTF DSP1012, *Boot Control Profile 1.0*,
32 https://www.dmtf.org/sites/default/files/standards/documents/DSP1012_1.0.pdf

33 DMTF DSP1013, *Fan Profile 1.0*,
34 https://www.dmtf.org/sites/default/files/standards/documents/DSP1013_1.0.pdf

35 DMTF DSP1014, *Ethernet Port Profile, 1.0*,
36 http://www.dmtf.org/standards/published_documents/DSP1014_1.0.pdf

37 DMTF DSP1015, *Power Supply Profile 1.0*,
38 https://www.dmtf.org/sites/default/files/standards/documents/DSP1015_1.0.pdf

- 39 DMTF DSP1015, *Power Supply Profile, 1.1*,
40 https://www.dmtf.org/sites/default/files/standards/documents/DSP1015_1.1.pdf
- 41 DMTF DSP1016, *Telnet Service Profile, 1.0*,
42 https://www.dmtf.org/sites/default/files/standards/documents/DSP1016_1.0.pdf
- 43 DMTF DSP1017, *SSH Service Profile, 1.0*,
44 https://www.dmtf.org/sites/default/files/standards/documents/DSP1017_1.0.pdf
- 45 DMTF DSP1018, *Service Processor Profile, 1.1*,
46 http://www.dmtf.org/standards/published_documents/DSP1018_1.1.pdf
- 47 DMTF DSP1022, *CPU Profile 1.0*,
48 https://www.dmtf.org/sites/default/files/standards/documents/DSP1022_1.0.pdf
- 49 DMTF DSP1023, *Software Inventory Profile 1.0*,
50 https://www.dmtf.org/sites/default/files/standards/documents/DSP1023_1.0.pdf
- 51 [DMTF DSP1024, *Text Console Redirection Profile 1.0*,](https://www.dmtf.org/sites/default/files/standards/documents/DSP1024_1.0.pdf)
52 http://www.dmtf.org/standards/published_documents/DSP1024_1.0.pdf
- 53 DMTF DSP1025, *Software Update Profile 1.0*,
54 https://www.dmtf.org/sites/default/files/standards/documents/DSP1025_1.0.pdf
- 55 DMTF DSP1026, *System Memory Profile 1.0*,
56 https://www.dmtf.org/sites/default/files/standards/documents/DSP1026_1.0.pdf
- 57 DMTF DSP1027, *Power State Management Profile 1.0*,
58 http://www.dmtf.org/standards/published_documents/DSP1027_1.0.pdf
- 59 DMTF DSP1027, *Power State Management Profile 2.0*,
60 http://www.dmtf.org/standards/published_documents/DSP1027_2.0.pdf
- 61 DMTF DSP1029, *OS Status Profile 1.0*,
62 https://www.dmtf.org/sites/default/files/standards/documents/DSP1029_1.0.pdf
- 63 DMTF DSP1029, *OS Status Profile, 1.1*,
64 https://www.dmtf.org/sites/default/files/standards/documents/DSP1029_1.1.pdf
- 65 DMTF DSP1030, *Battery Profile 1.0*,
66 https://www.dmtf.org/sites/default/files/standards/documents/DSP1030_1.0.pdf
- 67 DMTF DSP1033, *Profile Registration Profile 1.0*,
68 http://www.dmtf.org/standards/published_documents/DSP1033_1.0.pdf
- 69 DMTF DSP1033, *Profile Registration Profile 1.1*,
70 http://www.dmtf.org/standards/published_documents/DSP1033_1.1.pdf
- 71 DMTF DSP1034, *Simple Identity Management Profile 1.0*,
72 https://www.dmtf.org/sites/default/files/standards/documents/DSP1034_1.0.pdf
- 73 DMTF DSP1035, *Host LAN Network Port Profile 1.0*,
74 http://www.dmtf.org/standards/published_documents/DSP1035_1.0.pdf
- 75 DMTF DSP1036, *IP Interface Profile 1.0*,
76 http://www.dmtf.org/standards/published_documents/DSP1036_1.0.pdf
- 77 DMTF DSP1037, *DHCP Client Profile 1.0*,
78 http://www.dmtf.org/standards/published_documents/DSP1037_1.0.pdf
- 79 DMTF DSP1038, *DNS Client Profile 1.0*,
80 http://www.dmtf.org/standards/published_documents/DSP1038_1.0.pdf

- 81 DMTF DSP1039, *Role Based Authorization Profile 1.0*,
82 http://www.dmtf.org/standards/published_documents/DSP1039_1.0.pdf
- 83 DMTF DSP1040, *Watchdog Profile, 1.0*,
84 https://www.dmtf.org/sites/default/files/standards/documents/DSP1040_1.0.pdf
- 85 DMTF DSP1054, *Indications Profile 1.0*,
86 https://www.dmtf.org/sites/default/files/standards/documents/DSP1054_1.0.pdf
- 87 DMTF DSP1058, *Base Desktop and Mobile Profile 1.0*,
88 http://www.dmtf.org/standards/published_documents/DSP1058_1.0.pdf
- 89 DMTF DSP1061, *BIOS Management Profile 1.0*,
90 http://www.dmtf.org/standards/published_documents/DSP1061_1.0.pdf
- 91 DMTF DSP1070, *Opaque Management Data Profile 1.0*,
92 http://www.dmtf.org/standards/published_documents/DSP1070_1.0.pdf
- 93 DMTF DSP1074, *Indicator LED Profile, 1.0*,
94 http://www.dmtf.org/standards/published_documents/DSP1074_1.0.pdf
- 95 DMTF DSP1075, *PCI Device Profile, 1.0*,
96 https://www.dmtf.org/sites/default/files/standards/documents/DSP1075_1.0.pdf
- 97 DMTF DSP1076, *KVM Redirection 1.0*,
98 https://www.dmtf.org/sites/default/files/standards/documents/DSP1076_1.0.pdf
- 99 DMTF DSP1077, *USB Redirection Profile 1.0*,
100 https://www.dmtf.org/sites/default/files/standards/documents/DSP1077_1.0.pdf
- 101 DMTF DSP1086, *Media Redirection Profile 1.0*,
102 http://www.dmtf.org/standards/published_documents/DSP1086_1.0.pdf
- 103 DMTF DSP1108, *Physical Computer System View Profile, 1.0*,
104 http://www.dmtf.org/standards/published_documents/DSP1108_1.0.pdf
- 105 DMTF DSP1116, *IP Configuration Profile, 1.0*,
106 http://www.dmtf.org/standards/published_documents/DSP1116_1.0.pdf
- 107 DMTF DSP8007 *Platform Message Registry 1.0*,
108 http://schemas.dmtf.org/wbem/messageregistry/1/dsp8007_1.0.xml
- 109 DMTF DSP8030, DASH Namespace Schema 1.0, <http://schemas.dmtf.org/wbem/dash/1/dash.xsd>
- 110 IETF RFC 2246, T. Dierks et al., *The TLS Protocol Version 1.0*, <http://www.ietf.org/rfc/rfc2246.txt>
- 111 IETF RFC 4106, J. Viega and D. McGrew, *The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)*, <http://www.rfc-editor.org/rfc/rfc4106.txt>
- 112
- 113 IETF RFC 4301, S. Kent, *Security Architecture for the Internet Protocol*,
114 <http://www.rfc-editor.org/rfc/rfc4301.txt>
- 115 IETF RFC 4303, S. Kent, *IP Encapsulating Security Payload*, <http://www.ietf.org/rfc/rfc4303.txt>
- 116 IETF RFC 4346, T. Dierks et al., *The TLS Protocol Version 1.1*, <http://www.ietf.org/rfc/rfc4346.txt>
- 117 IETF RFC 5246, T. Dierks et al., *The TLS Protocol Version 1.2*, <http://www.ietf.org/rfc/rfc5246.txt>
- 118 IETF RFC 8446, E. Rescorla et al., *The TLS Protocol Version 1.3*, <https://www.ietf.org/rfc/rfc8446.txt>
- 119 ISO/IEC Directives, Part 2, *Rules for the structure and drafting of International Standards*,
120 <http://isotc.iso.org/livelink/livelink.exe?func=ll&objId=4230456&objAction=browse&sort=subtype>

121 3 Terms and definitions

122 In this document, some terms have a specific meaning beyond the normal English meaning. Those terms
123 are defined in this clause.

124 The terms "shall" ("required"), "shall not", "should" ("recommended"), "should not" ("not recommended"),
125 "may", "need not" ("not required"), "can" and "cannot" in this document are to be interpreted as described
126 in [ISO/IEC Directives, Part 2](#), Clause 7. The terms in parentheses are alternatives for the preceding term,
127 for use in exceptional cases when the preceding term cannot be used for linguistic reasons. Note that
128 [ISO/IEC Directives, Part 2](#), Clause 7 specifies additional alternatives. Occurrences of such additional
129 alternatives shall be interpreted in their normal English meaning.

130 The terms "clause", "subclause", "paragraph", and "annex" in this document are to be interpreted as
131 described in [ISO/IEC Directives, Part 2](#), Clause 6.

132 The terms "normative" and "informative" in this document are to be interpreted as described in [ISO/IEC](#)
133 [Directives, Part 2](#), Clause 3. In this document, clauses, subclauses, or annexes labeled "(informative)" do
134 not contain normative content. Notes and examples are always informative elements.

135 The terms defined in [DSP0004](#), [DSP0223](#), and [DSP1001](#) apply to this document. The following additional
136 terms are used in this document.

137 3.1

138 **can**

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

140 3.2

141 **cannot**

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

143 3.3

144 **conditional**

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

147 3.4

148 **mandatory**

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

151 3.5

152 **may**

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

154 3.6

155 **need not**

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

157 3.7

158 **optional**

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

- 160 **3.8**
161 **shall**
162 indicates requirements to be followed strictly in order to conform to the document and from which no
163 deviation is permitted
- 164 **3.9**
165 **shall not**
166 indicates requirements to be followed in order to conform to the document and from which no deviation is
167 permitted
- 168 **3.10**
169 **should**
170 indicates that among several possibilities, one is recommended as particularly suitable, without
171 mentioning or excluding others, or that a certain course of action is preferred but not necessarily required
- 172 **3.11**
173 **should not**
174 indicates that a certain possibility or course of action is deprecated but not prohibited

175 **4 Symbols and abbreviated terms**

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

- 177 **4.1**
178 **ASF**
179 Alert Standard Format
- 180 **4.2**
181 **IANA**
182 Internet Assigned Numbers Authority
- 183 **4.3**
184 **IP**
185 Internet Protocol
- 186 **4.4**
187 **MAC**
188 Media Access Control
- 189 **4.5**
190 **MAP**
191 Management Access Point
- 192 **4.6**
193 **RMCP**
194 Remote Management and Control Protocol
- 195 **4.7**
196 **TCP**
197 Transmission Control Protocol

- 198 **4.8**
- 199 **TLS**
- 200 Transport Layer Security
- 201 **4.9**
- 202 **UDP**
- 203 User Datagram Protocol
- 204 **4.10**
- 205 **URI**
- 206 Uniform Resource Identifier
- 207 **4.11**
- 208 **WS**
- 209 Web Services

210 **5 Mandatory profiles and specifications**

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

213 **Table 1 – Mandatory profiles and specifications**

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

214 **6 Optional profiles**

215 The optional profiles shown in Table 2 may be implemented. When a profile in Table 2 is implemented,
 216 the requirements specified in this clause shall be met. For an optional profile with multiple versions
 217 listed in the table below, one or more versions of the optional profile may be implemented.
 218 If implemented, the latest version of the optional profile should be implemented.

219 **Table 2 – Optional profiles**

Name	Number	Version	Description
<i>Battery Profile</i>	DSP1030	1.0	
<i>BIOS Management Profile</i>	DSP1061	1.0	
<i>Boot Control Profile</i>	DSP1012	1.0	
<i>CPU Profile</i>	DSP1022	1.0	
<i>DHCP Client Profile</i>	DSP1037	1.0	
<i>DNS Client Profile</i>	DSP1038	1.0	
<i>Ethernet Port Profile</i>	DSP1014	1.0	
<i>Fan Profile</i>	DSP1013	1.0	
<i>Host LAN Network Port Profile</i>	DSP1035	1.0	
<i>Indications Profile</i>	DSP1054	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> (DSP8007). 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 DSP4006 .
<i>Indicator LED Profile</i>	DSP1074	1.0	
<i>IP Interface Profile</i>	DSP1036	1.0	
<i>IP Configuration Profile</i>	DSP1116	1.0	
<i>KVM Redirection Profile</i>	DSP1076	1.0	
<i>Media Redirection Profile</i>	DSP1086	1.0	
<i>Opaque Management Data Profile</i>	DSP1070	1.0	
<i>OS Status Profile</i>	DSP1029	1.0	
<i>OS Status Profile</i>	DSP1029	1.1	
<i>PCI Device Profile</i>	DSP1075	1.0	
<i>Physical Asset Profile</i>	DSP1011	1.0	
<i>Physical Computer System View Profile</i>	DSP1108	1.0	
<i>Power State Management Profile</i>	DSP1027	1.0	
<i>Power State Management Profile</i>	DSP1027	2.0	
<i>Power Supply Profile</i>	DSP1015	1.0	
<i>Power Supply Profile</i>	DSP1015	1.1	

Name	Number	Version	Description
Profile Registration Profile	DSP1033	1.1	
Record Log Profile	DSP1010	2.0	
Sensors Profile	DSP1009	1.0	
Sensors Profile	DSP1009	1.1	
Service Processor Profile	DSP1018	1.1	
Software Inventory Profile	DSP1023	1.0	
Software Update Profile	DSP1025	1.0	
SSH Service Profile	DSP1017	1.0	
System Memory Profile	DSP1026	1.0	
Telnet Service Profile	DSP1016	1.0	
Text Console Redirection Profile	DSP1024	1.0	
USB Redirection Profile	DSP1077	1.0	
Watchdog Profile	DSP1040	1.0	

220 7 Protocol implementation requirements

221 A DASH-compliant implementation shall use a CIM-based data model for representing managed
 222 resources and services. This clause describes the Management Protocol and Transport Protocol
 223 requirements for a DASH implementation.

224 7.1 Management protocol

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

228 7.1.1 XML namespaces

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

230 (1) `http://schemas.dmtf.org/wbem/dash/1/dash.xsd`

231 7.1.2 WS-Transfer

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

234

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.

235 7.1.3 WS-Enumeration

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

239

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 DSP0226 . Implementation of this operation is not recommended.
GetStatus	Optional	See Rule R8.1-4 in DSP0226 . 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 DSP0226 . Implementation of this operation is not recommended.

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

243 7.1.3.1 WS-Enumeration filter dialects

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

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

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

251 **7.1.4 WS-Eventing**

252 Support for WS-Eventing is conditional.

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

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

Operation	Requirement	Notes
Subscribe	Mandatory	
Renew	Mandatory	
Unsubscribe	Mandatory	
SubscriptionEnd	Optional	
GetStatus	Optional	See Rule R10.3-1 in DSP0226 . Implementation of this operation is not recommended.

257 **7.1.4.1 WS-Eventing messaging security**

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

259 **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 clause 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 clause 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

260 7.1.4.2 WS-Eventing delivery mode

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

264 7.1.4.3 Subscription related property definition guidance

265 The PersistenceType property in a CIM_ListenerDestination instance created internally in response to
266 wse:Subscribe should be set to 3 (Transient).

267 The value for the FailureTriggerTimeInterval property on the CIM_IndicationSubscription or
268 CIM_FilterCollectionSubscription instance created internally in response to wse:Subscribe should be to
269 30 seconds.

270 7.2 Transport protocol

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

274 8 Security implementation requirements

275 This clause describes transport requirements, roles and authorization, user account management, and
276 authentication.

277 8.1 Transport requirements

278 DASH defines two security classes for HTTP 1.1 transport:

279 1) **Class A:** The security class A requires HTTP digest authentication for the user authentication.
280 For this class, no encryption capabilities are required beyond the encryption of the password
281 during the digest authentication exchange. If class A is implemented, one of either MD5 digest
282 algorithm or SHA-256 digest algorithm shall be supported.

283 • **String = "HTTP_DIGEST"**

284 • **String = "HTTP_DIGEST_SHA256"**

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

288 • **String = "HTTP_TLS_1"**

289 • TLS_RSA_WITH_AES_128_CBC_SHA (for TLS) and MD5 (for HTTP digest)

290 • **String = "HTTP_TLS_2"**

291 • TLS_RSA_WITH_AES_128_CBC_SHA

292 • **String = "HTTP_TLS_3"**

293 • TLS 1.2 (TLS_DHE_RSA_WITH_AES_128_CBC_SHA256), Digest SHA-256

294 • **String = "HTTP_TLS_4"**

295 TLS 1.3 or later (TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256), Digest SHA-256

296 For Key Exchange: ECDHE secp256r1

297 For Signature Authentication: rsa_pss_rsae_sha256

298 For Symmetric Cipher (Record Layer): TLS_AES_128_GCM_SHA256

- String = "HTTP_IPSEC"

A DASH implementation may support Class A. A DASH implementation shall support Class B security class for privacy/confidentiality and additional security.

For class B compliance, the DASH implementation shall support at least one of the security profiles HTTP_TLS_1, HTTP_TLS_2, HTTP_TLS_3, HTTP_TLS_4 or HTTP_IPSEC. For enhanced security, the implementation should support either "HTTP_TLS_3" or "HTTP_TLS_4" security profiles.

Refer to 7.1.4.1 for WS-Eventing security requirements.

Refer to 9.2.2 Table 11 for URI identifying the security profiles.

8.1.1 Cryptographic algorithms and cipher suites

Table 7 lists the required cryptographic algorithms or cipher suites for the security profiles mentioned in this clause.

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 1.2 or later Refer to RFC 2246, RFC 4346, RFC 5246 and RFC 3268.
"HTTP_TLS_2"	TLS_RSA_WITH_AES_128_CBC_SHA	TLS version 1.2 or later Refer to RFC 2246, RFC 4346, RFC 5246 and RFC 3268.
"HTTP_TLS_3"	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 and SHA-256 (for HTTP digest)	TLS version 1.2 Refer to RFC 5246, RFC 3268 and RFC 7616
"HTTP_TLS_4"	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 and SHA-256 (for HTTP digest) For Key Exchange: ECDHE secp256r1 For Signature Authentication: rsa_pss_rsae_sha256 For Symmetric Cipher (Record Layer): TLS_AES_128_GCM_SHA256	TLS version 1.3 or later Refer to RFC 8446
"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 4301 , 4303 , and 4106

Cryptographic protocols TLS 1.0 and TLS 1.1 are deprecated.

312 8.2 Roles and authorization

313 Table 8 outlines the Operational Roles supported by DASH implementations and the respective DASH
314 requirements.

315 **Table 8 – Operational Roles Supported by DASH**

Operational Role	Requirement	Notes
Read-only User	Optional	For detailed description of these roles see DSP2014 .
Operator	Optional	
Administrator	Mandatory	

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

319 8.3 User account management

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

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

325 **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

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

329 8.4 Authentication mechanisms

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

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

334 **Table 10 – Authentication mechanisms**

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

335 9 Discovery requirements

336 Multiple discovery stages are required to accumulate the necessary information from the managed
337 system. This clause defines the implementation requirements of the stages involved in discovering
338 managed systems and their management capabilities.

339 9.1 Network endpoint discovery stage

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

343 9.2 Management access point discovery stage

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

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

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

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

348 9.2.1 RMCP Presence Ping/Pong

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

352 The format of the RMCP Presence Pong (40h) data clause shall conform to clause 3.2.4.3 of [DSP0136](#)
353 with the following definition:

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

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

357 9.2.2 WS-Management identify method

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

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

```

363 <s:Body>
364   <wsmid:IdentifyResponse>
365     <wsmid:ProtocolVersion> xs:anyURI </wsmid:ProtocolVersion>
366     <wsmid:ProductVendor> xs:string </wsmid:ProductVendor>
367     <wsmid:ProductVersion> xs:string </wsmid:ProductVersion>
368     <dash:DASHVersion> xs:string </dash:DASHVersion>
369     <wsmid:SecurityProfiles>
370       <wsmid:SecurityProfileName> xs:string or URI </wsmid:SecurityProfileName> +
371     </wsmid:SecurityProfiles>
372   </wsmid:IdentifyResponse>
373 </s:Body>
    
```

374 Table 11 defines the *IdentifyResponse* payload requirements for DASH 1.1.

375 **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 DSP0226 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 Class A: "HTTP_DIGEST": http://schemas.dmtf.org/wbem/wsman/1/wsman/secprofile/http/digest "HTTP_DIGEST_SHA256": http://schemas.dmtf.org/wbem/wsman/1/wsman/secprofile/http/digest_sha256 Class B: "HTTP_TLS_1": http://schemas.dmtf.org/wbem/wsman/1/wsman/secprofile/https/digest "HTTP_TLS_2": http://schemas.dmtf.org/wbem/wsman/1/wsman/secprofile/https/basic "HTTP_TLS_3": http://schemas.dmtf.org/wbem/wsman/1/wsman/secprofile/https/digest_t3 "HTTP_TLS_4": http://schemas.dmtf.org/wbem/wsman/1/wsman/secprofile/https/digest_t4 "HTTP_IPSEC": http://schemas.dmtf.org/wbem/wsman/1/wsman/secprofile/http/digest/ipsec

376 **9.2.3 wsmid:Identify security implementation requirements**

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

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

381 **9.3 Enumeration of management capabilities stage**

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

386 **9.4 RegisteredSpecification instance**

387 The DASH implementation should support an instance of CIM_RegisteredSpecification to indicate
 388 support for this version of the specification.

389 Table 12 identifies the element requirements for CIM_RegisteredSpecification.

390

Table 12 – CIM_RegisteredSpecification element requirements

Element	Requirement	Description
Properties		
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 "1.3.1".
AdvertiseTypes	Mandatory	Required, see Schema definition.
AdvertiseTypeDescriptions	Mandatory	See Schema definition.
Operations		
GetInstance	Mandatory	
EnumerateInstances	Mandatory	
EnumerateInstanceNames	Mandatory	

391

392 The instance of CIM_RegisteredSpecification shall be exposed in the interop namespace. The instance to
 393 CIM_RegisteredSpecification shall be associated with at least one instance of CIM_RegisteredProfile of
 394 one of the mandatory profiles defined in this specification using an instance of
 395 CIM_ReferencedSpecification. The Antecedent property of the instance of CIM_ReferencedSpecification
 396 shall reference the instance of the CIM_RegisteredProfile. The Dependent property of the instance of
 397 CIM_ReferencedSpecification shall reference the instance CIM_RegisteredSpecification.

398 10 In-band and out-of-band traffic requirements

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

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

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

- 406 • Sideband: TCP ports for WS-Management Service
 - 407 – OOB-WS-HTTP
 - 408 – TCP 623
 - 409 – OOB-WS-HTTPS
 - 410 – TCP 664 (If class B is implemented)
- 411 • In-band: TCP ports for WS-Management Service may be supported on the following transport
 412 ports and shall be transport specific:

- 413 – HTTP
- 414 – HTTPS (If class B is implemented)

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

416
417
418

ANNEX A (informative) Change log

Version	Date	Description
1.0.0	2009-05-19	
1.0.1	2009-10-16	Updated
1.1.0	2009-06-22	DMTF Standard Release
1.2.0	2014-12-22	DMTF Standard Release
1.2.1	2015-05-21	DMTF Standard Release
1.3.0	2021-01-08	Added TLS security enhancements.
1.3.1	2022-01-01	Reference to added Profile Registration Profile 1.1

419

Bibliography

420

421 DMTF DSP2014, *Systems Management Architecture for Mobile and Desktop Hardware White Paper*
422 1.1.0, http://www.dmtf.org/standards/published_documents/DSP2014_1.1.0.pdf
423 (Informative text in this document details Protocol, Security, and Discovery.)

424 DMTF DSP4006, Standard Registry Development and Publication Process 1.1,
425 http://www.dmtf.org/standards/published_documents/DSP4006_1.1.0.pdf