



1
2
3
4

Document Number: DSP0232

Date: 2009-10-16

Version: 1.0.1

5 **DASH Implementation Requirements**

6 **Document Type: Specification**
7 **Document Status: DMTF Standard**
8 **Document Language: E**
9

10 Copyright Notice

11 Copyright © 2009 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26 withdrawn or modified after publication, and shall be indemnified and held harmless by any party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

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..... 8

40 3 Terms and Definitions 8

41 4 Symbols and Abbreviated Terms..... 9

42 5 Mandatory Profiles and Specifications 10

43 6 Optional Profiles 11

44 7 Protocol Implementation Requirements 11

45 7.1 Management Protocol..... 11

46 7.2 Transport Protocol 14

47 8 Security Implementation Requirements 14

48 8.1 Transport Requirements 14

49 8.2 Roles and Authorization..... 15

50 8.3 User Account Management 15

51 8.4 Authentication Mechanisms 16

52 9 Discovery Requirements 16

53 9.1 Network Endpoint Discovery Stage 16

54 9.2 Management Access Point Discovery Stage..... 17

55 9.3 Enumeration of Management Capabilities Stage 18

56 10 In-Band and Out-of-Band Traffic Requirements 18

57 ANNEX A (informative) Change Log..... 20

58 ANNEX B (informative) HTTP Status Codes 21

59 Bibliography 22

60

61 Tables

62 Table 1 – Mandatory Profiles and Specifications..... 10

63 Table 2 – Optional Profiles..... 11

64 Table 3 – WS-Transfer Operations 12

65 Table 4 – WS-Enumeration Operations 12

66 Table 5 – WS-Eventing Operations 13

67 Table 6 – WS-Eventing Message Security Recommendations 13

68 Table 7- Required Cryptographic Algorithms or Cipher Suites..... 15

69 Table 8 – Operational Roles Supported by DASH..... 15

70 Table 9 – User Account Operations..... 15

71 Table 10 – Authentication Mechanisms 16

72 Table 11 – WS-Management IdentifyResponse Payload Elements 17

73

75

Foreword

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

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

80 **Acknowledgments**

81 The authors wish to acknowledge the following people.

82 **Editors:**

- 83 • Joe Kozlowski – Dell Inc.
- 84 • Steven Breed – Dell Inc.

85 **Contributors:**

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

101

102

Introduction

103 This specification describes the conformance requirements for implementing the Desktop and Mobile
104 Architecture for System Hardware (DASH) version 1.0.

105

DASH Implementation Requirements

106 1 Scope

107 This document describes the requirements for implementing the Desktop and Mobile Architecture for
108 System Hardware version 1.0. This document does not define the implementation requirements directly.
109 In clause 5, the mandatory specifications to be implemented are defined. In clauses 6, 7, 8, 9, and 10 the
110 optional and conditional specifications are defined.

111 2 Normative References

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

115 2.1 Approved References

- 116 DMTF DSP0136, *Alert Standard Format Specification 2.0*,
117 <http://www.dmtf.org/standards/documents/ASF/DSP0136.pdf>
- 118 DMTF DSP0226, *Web Services for Management 1.0*,
119 http://www.dmtf.org/standards/published_documents/DSP0226_1.0.pdf
- 120 DMTF DSP0227, *WS-Management — CIM Binding Specification 1.0*,
121 http://www.dmtf.org/standards/published_documents/DSP0227_1.0.pdf
- 122 DMTF DSP0230, *WS-CIM Mapping Specification 1.0*,
123 http://www.dmtf.org/standards/published_documents/DSP0230_1.0.pdf
- 124 DMTF DSP1009, *Sensors Profile 1.0*,
125 http://www.dmtf.org/standards/published_documents/DSP1009_1.0.pdf
- 126 DMTF DSP1011, *Physical Asset Profile 1.0*,
127 http://www.dmtf.org/standards/published_documents/DSP1011_1.0.pdf
- 128 DMTF DSP1012, *Boot Control Profile 1.0*,
129 http://www.dmtf.org/standards/published_documents/DSP1012_1.0.pdf
- 130 DMTF DSP1013, *Fan Profile 1.0*,
131 http://www.dmtf.org/standards/published_documents/DSP1013_1.0.pdf
- 132 DMTF DSP1015, *Power Supply Profile 1.0*,
133 http://www.dmtf.org/standards/published_documents/DSP1015_1.0.pdf
- 134 DMTF DSP1022, *CPU Profile 1.0*,
135 http://www.dmtf.org/standards/published_documents/DSP1022_1.0.pdf
- 136 DMTF DSP1023, *Software Inventory Profile 1.0*,
137 http://www.dmtf.org/standards/published_documents/DSP1023_1.0.pdf
- 138 DMTF DSP1026, *System Memory Profile 1.0*,
139 http://www.dmtf.org/standards/published_documents/DSP1026_1.0.pdf
- 140 DMTF DSP1027, *Power State Management Profile 1.0*,
141 http://www.dmtf.org/standards/published_documents/DSP1027_1.0.pdf

- 142 DMTF DSP1033, *Profile Registration Profile 1.0*,
143 http://www.dmtf.org/standards/published_documents/DSP1033_1.0.pdf
- 144 DMTF DSP1034, *Simple Identity Management Profile 1.0*,
145 http://www.dmtf.org/standards/published_documents/DSP1034_1.0.pdf
- 146 DMTF DSP1039, *Role Based Authorization Profile 1.0*,
147 http://www.dmtf.org/standards/published_documents/DSP1039_1.0.pdf
- 148 DMTF DSP1054, *Indications Profile 1.0*,
149 http://www.dmtf.org/standards/published_documents/DSP1054_1.0.pdf
- 150 DMTF DSP1058, *Base Desktop and Mobile Profile 1.0*,
151 http://www.dmtf.org/standards/published_documents/DSP1058_1.0.pdf
- 152 DMTF DSP8007 *Platform Message Registry 1.0*,
153 <http://schemas.dmtf.org/wbem/messageregistry/1/dsp8007.xml>
- 154 IETF RFC 2246, T. Dierks et al., *The TLS Protocol Version 1.0*, <http://www.ietf.org/rfc/rfc2246.txt>
- 155 IETF RFC 3268, P. Chown, *Advanced Encryption Standard (AES) Ciphersuites for Transport Layer
156 Security (TLS)*, <http://www.ietf.org/rfc/rfc3268.txt>
- 157 IETF RFC 4301, S. Kent, *Security Architecture for the Internet Protocol*,
158 <http://www.rfc-editor.org/rfc/rfc4301.txt>
- 159 IETF RFC 4303, S. Kent, *IP Encapsulating Security Payload*, <http://www.ietf.org/rfc/rfc4303.txt>
- 160 IETF RFC 4106, J. Viega and D. McGrew, *The Use of Galois/Counter Mode (GCM) in IPsec
161 Encapsulating Security Payload (ESP)*, <http://www.rfc-editor.org/rfc/rfc4106.txt>

162 **2.2 Other References**

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

165 **3 Terms and Definitions**

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

167 **3.1**

168 **can**

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

170 **3.2**

171 **cannot**

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

173 **3.3**

174 **conditional**

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

177 **3.4**

178 **mandatory**

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

- 181 **3.5**
182 **may**
183 indicates a course of action permissible within the limits of the document
- 184 **3.6**
185 **need not**
186 indicates a course of action permissible within the limits of the document
- 187 **3.7**
188 **optional**
189 indicates a course of action permissible within the limits of the document
- 190 **3.8**
191 **shall**
192 indicates requirements to be followed strictly in order to conform to the document and from which no
193 deviation is permitted
- 194 **3.9**
195 **shall not**
196 indicates requirements to be followed in order to conform to the document and from which no deviation is
197 permitted
- 198 **3.10**
199 **should**
200 indicates that among several possibilities, one is recommended as particularly suitable, without
201 mentioning or excluding others, or that a certain course of action is preferred but not necessarily required
- 202 **3.11**
203 **should not**
204 indicates that a certain possibility or course of action is deprecated but not prohibited

205 **4 Symbols and Abbreviated Terms**

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

- 207 **4.1**
208 **ASF**
209 Alert Standard Format
- 210 **4.2**
211 **IANA**
212 Internet Assigned Numbers Authority
- 213 **4.3**
214 **IP**
215 Internet Protocol
- 216 **4.4**
217 **MAC**
218 Media Access Control

- 219 **4.5**
 220 **MAP**
 221 Management Access Point
- 222 **4.6**
 223 **RMCP**
 224 Remote Management and Control Protocol
- 225 **4.7**
 226 **TCP**
 227 Transmission Control Protocol
- 228 **4.8**
 229 **TLS**
 230 Transport Layer Security
- 231 **4.9**
 232 **UDP**
 233 User Datagram Protocol
- 234 **4.10**
 235 **URI**
 236 Uniform Resource Identifier
- 237 **4.11**
 238 **WS**
 239 Web Services

240 **5 Mandatory Profiles and Specifications**

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

243 **Table 1 – Mandatory Profiles and Specifications**

| Name | Number | Version | Description |
|--|-------------------------|---------|-------------|
| <i>Base Desktop and Mobile Profile</i> | DSP1058 | 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 | |
| <i>Role Based Authorization Profile</i> | DSP1039 | 1.0 | |
| <i>Simple Identity Management Profile</i> | DSP1034 | 1.0 | |
| <i>Profile Registration Profile</i> | DSP1033 | 1.0 | |

244 6 Optional Profiles

245 The optional profiles shown in Table 2 may be implemented. When a profile is implemented, the
246 requirements specified in this section shall be met.

247 **Table 2 – Optional Profiles**

| Name | Number | Version | Description |
|---------------------------------------|-------------------------|---------|---|
| <i>Boot Control Profile</i> | DSP1012 | 1.0 | |
| <i>CPU Profile</i> | DSP1022 | 1.0 | |
| <i>Fan Profile</i> | DSP1013 | 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. |
| <i>Physical Asset Profile</i> | DSP1011 | 1.0 | |
| <i>Power State Management Profile</i> | DSP1027 | 1.0 | |
| <i>Power Supply Profile</i> | DSP1015 | 1.0 | |
| <i>Sensors Profile</i> | DSP1009 | 1.0 | |
| <i>Software Inventory Profile</i> | DSP1023 | 1.0 | |
| <i>System Memory Profile</i> | DSP1026 | 1.0 | |

248 7 Protocol Implementation Requirements

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

252 7.1 Management Protocol

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

256 7.1.1 XML Namespaces

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

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

259 7.1.2 WS-Transfer

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

262

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. |

263 7.1.3 WS-Enumeration

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

267

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. |

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

271 7.1.3.1 WS-Enumeration Filter Dialects

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

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

277 It is optional for DASH implementations to support the CQL filter dialect for enumeration as described in
 278 clause 8.1 of [DSP0227](#). This clause does not contravene Rule R8.2.1-5 of [DSP0226](#).

279 **7.1.4 WS-Eventing**

280 Support for WS-Eventing is conditional. A service advertising conformance to the *Indications Profile*
 281 ([DSP1054](#)) shall support WS-Eventing as described in clause 10 of [DSP0226](#) and further constrained by
 282 the definition described in this section 7.1.4. Table 5 defines support for WS-Eventing operations and
 283 their respective DASH requirements.

284 **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. |

285 **7.1.4.1 WS-Eventing Messaging Security**

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

287 **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 |

288 7.1.4.2 WS-Eventing Delivery Mode

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

292 7.1.4.3 Subscription Related Property Definition Guidance

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

295 The value for the FailureTriggerTimeInterval property on the CIM_IndicationSubscription or
296 CIM_FilterCollectionSubscription instance created internally in response to wse:Subscribe should be to
297 30 seconds.

298 7.2 Transport Protocol

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

302 8 Security Implementation Requirements

303 This section describes transport requirements, roles and authorization, user account management, and
304 authentication.

305 8.1 Transport Requirements

306 DASH defines two security classes for HTTP 1.1 transport:

- 307 1) **Class A:** The security class A requires HTTP digest authentication for the user authentication.
308 For this class, no encryption capabilities are required beyond the encryption of the password
309 during the digest authentication exchange. If class A is implemented, MD5 digest algorithm shall
310 be supported. The SHA-1 digest algorithm may be supported.
- 311 • String = "HTTP_DIGEST"
 - 312 – URI = <http://schemas.dmtf.org/wbem/wsman/1/wsman/secprofile/http/digest>
 - 313 2) **Class B:** This class defines three security profiles that are based on either TLS or IPsec with
314 specifically selected modes and cryptographic algorithms. For class B compliance, the support
315 for at least one of the following security profiles is mandatory:
 - 316 • String = "HTTP_TLS_1"
 - 317 – URI = <http://schemas.dmtf.org/wbem/wsman/1/wsman/secprofile/https/digest>
 - 318 • String = "HTTP_TLS_2"
 - 319 – URI = <http://schemas.dmtf.org/wbem/wsman/1/wsman/secprofile/https/basic>
 - 320 • String = "HTTP_IPSEC"
 - 321 For this profile IPsec provides both machine-level authentication and encryption services
322 and HTTP digest provides user-level authentication.
 - 323 – URI = <http://schemas.dmtf.org/wbem/wsman/1/wsman/secprofile/http/digest/ipsec>

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

326 Refer to 7.1.4.1 for WS-Eventing security requirements.

327 **8.1.1 Cryptographic Algorithms and Cipher Suites**

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

330 **Table 7- Required Cryptographic Algorithms or Cipher Suites**

| Security Profile | Required Algorithm(s) or Cipher suite | Notes |
|------------------|---|---|
| "HTTP_DIGEST" | MD5 | SHA- is optional. |
| "HTTP_TLS_1" | TLS_RSA_WITH_AES_128_CBC_SHA | TLS version 1.0 Refer to RFC 3268 and 2246 . |
| "HTTP_TLS_2" | TLS_RSA_WITH_AES_128_CBC_SHA | TLS version 1.0 Refer to RFC 3268 and 2246 . |
| "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 RFC 4301 , 4303 , and 4106 . |

331 **8.2 Roles and Authorization**

332 Table 8 outlines the Operational Roles supported by DASH implementations and the respective DASH
 333 requirements.

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

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

335 A DASH-compliant service shall support the administrator role. An implementation may support the
 336 operator and/or read-only user roles.

337 **8.3 User Account Management**

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

340 Each user shall have the ability to modify its own account credentials. An account in the administrator role
 341 shall be able to perform account management for all users. Table 9 outlines the operations supported for
 342 user account management and the respective DASH requirements.

343 **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 |

| Operation | Requirement | Notes |
|---|-------------|--|
| 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 |

344 The modifications of privileges include the changing of bindings between accounts or groups and roles.

345 8.4 Authentication Mechanisms

346 DASH implementations shall support one or two levels of authentication.

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

349 **Table 10 – Authentication Mechanisms**

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

350 9 Discovery Requirements

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

354 9.1 Network Endpoint Discovery Stage

355 Section 8.2 of the *Desktop and Mobile Systems Management White Paper* ([DSP2014](#)) describes
356 endpoint discovery methods. A DASH 1.0 compliant implementation need not support any of the
357 described methods.

358 **9.2 Management Access Point Discovery Stage**

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

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

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

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

363 **9.2.1 RMCP Presence Ping/Pong**

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

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

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

370 A DASH-compliant MAP should support this command on the ASF-RMCP well-known UDP port (623).
 371 Support of Presence Ping/Pong on the ASF-Secure-RMCP well-known UDP port (664) is not
 372 recommended for a DASH service.

373 **9.2.2 WS-Management Identify Method**

374 Refer to clause 11 of [RFC 2246](#) for a definition of the Identify method. A DASH-compliant management
 375 service shall support the Identify method on each DASH access port that it supports.

376 In addition to the child element defined in [RFC 2246](#), the following extension elements are defined by
 377 DASH as children of the *IdentifyResponse* element:

```

378 4.1 <s:Body>
379   <wsmid:IdentifyResponse>
380     <wsmid:ProtocolVersion> xs:anyURI </wsmid:ProtocolVersion>
381     <wsmid:ProductVendor> xs:string </wsmid:ProductVendor>
382     <wsmid:ProductVersion> xs:string </wsmid:ProductVersion>
383     <dash:DASHVersion> xs:string </dash:DASHVersion>
384     <wsmid:SecurityProfiles>
385       <wsmid:SecurityProfileName> xs:string or URI </wsmid:SecurityProfileName> +
386     </wsmid:SecurityProfiles>
387   </wsmid:IdentifyResponse>
388 </s:Body>
    
```

389 Table 11 defines the IdentifyResponse payload requirements for DASH 1.0.

390 **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 | |

| Element | Requirement | Notes |
|---|-------------|---|
| wsmid:IdentifyResponse/wsmid:ProductVersion | Optional | |
| wsmid:IdentifyResponse/dash:DASHVersion | Mandatory | Identifies the DASH version supported, which shall be formatted as "n.n.n". Example: "1.0.0" |
| 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 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_IPSEC": http://schemas.dmtf.org/wbem/wsman/1/wsman/secprofile/http/digest |

391 9.2.3 wsmid:Identify Security Implementation Requirements

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

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

396 9.3 Enumeration of Management Capabilities Stage

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

401 10 In-Band and Out-of-Band Traffic Requirements

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

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

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

409 • Sideband DMTF Web Services Protocol Ports

410 – OOB-WS-HTTP

411 ▪ TCP 623

412 – OOB-WS-HTTPS (If class B is implemented)

413 ▪ TCP 664

414 • In-band Web Services Protocol Ports may be supported on the following transport ports and
415 shall be transport specific:

416 – HTTP

417 – HTTPS (If class B is implemented)

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

419
420
421
422
423

ANNEX A (informative)

Change Log

| Version | Date | Author | Description |
|----------------|-------------|---------------|-----------------------|
| 1.0.0 | 3/5/2009 | J. Kozlowski | DMTF Standard Release |
| 1.0.1 | 8/14/2009 | | DMTF Standard Release |

424
425
426
427
428

ANNEX B (informative)

HTTP Status Codes

429 This section is intended to direct implementers to the appropriate specifications for implementation
430 requirements surrounding HTTP status codes:

- 431 • [DSP0226](#) ANNEX C, line 4298; "RC.2-9: When delivering faults, an HTTP status code of 500
432 should be used in the response for s:Receiver faults, and a code of 400 should be used for
433 s:Sender faults."
- 434 • [WS-I Basic Profile](#) 4.3.9 "HTTP Server Error Status Codes
435 HTTP uses the 5xx series of status codes to indicate failure due to a server error.
436 R1126 An INSTANCE MUST use a "500 Internal Server Error" HTTP status code if the
437 response message is a SOAP Fault."

438 NOTE: If an implementation returns a HTTP 200 (OK), it will be handled by the HTTP libraries directly. Sometimes,
439 code using such libraries, only indicate that there is a fault, and do not return the fault itself.

440

441

Bibliography

442

443 DMTF DSP2014, *Systems Management Architecture for Mobile and Desktop Hardware White Paper*444 1.1.0, http://www.dmtf.org/standards/published_documents/DSP2014_1.1.0.pdf

445 (Informative text in this document details Protocol, Security, and Discovery.)

446