



Document Number: DSP0232

Date: 2009-06-22

Version: 1.1.0

DASH Implementation Requirements

Document Type: Specification

Document Status: DMTF Standard

Document Language: E

Copyright Notice

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

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

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patent owner or claimant, and shall have no liability or responsibility for costs or losses incurred if a standard is withdrawn or modified after publication, and shall be indemnified and held harmless by any party implementing the standard from any and all claims of infringement by a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

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

CONTENTS

Foreword	5
Introduction	6
1 Scope	7
2 Normative References.....	7
2.1 Approved References	7
2.2 Other References.....	9
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.....	17
8.3 User Account Management	17
8.4 Authentication Mechanisms	18
9 Discovery Requirements	18
9.1 Network Endpoint Discovery Stage	19
9.2 Management Access Point Discovery Stage.....	19
9.3 Enumeration of Management Capabilities Stage	21
10 In-Band and Out-of-Band Traffic Requirements	21
ANNEX A (informative) Change Log.....	22
Bibliography	23

Tables

Table 1 – Mandatory Profiles and Specifications.....	11
Table 2 – Optional Profiles.....	12
Table 3 – WS-Transfer Operations	13
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.....	17
Table 9 – User Account Operations.....	18
Table 10 – Authentication Mechanisms	18
Table 11 – WS-Management IdentifyResponse Payload Elements.....	20

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 authors wish to acknowledge the following people.

Editors:

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

Contributors:

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

Introduction

This specification describes the conformance requirements for implementing the Desktop and Mobile Architecture for System Hardware (DASH) version 1.1.

1

DASH Implementation Requirements

1 Scope

3 This document describes the requirements for implementing the Desktop and Mobile Architecture for
4 System Hardware version 1.1. 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
10 references, only the edition cited applies. For undated references, the latest edition of the referenced
11 document (including any amendments) applies.

2.1 Approved References

- 13 DMTF DSP0136, *Alert Standard Format Specification 2.0*,
14 http://www.dmtf.org/standards/documents/ASF/DSP0136_2.0.pdf
- 15 DMTF DSP0226, *Web Services for Management 1.0*,
16 http://www.dmtf.org/standards/published_documents/DSP0226_1.0.pdf
- 17 DMTF DSP0227, *WS-Management CIM Binding Specification 1.0*,
18 http://www.dmtf.org/standards/published_documents/DSP0227_1.0.pdf
- 19 DMTF DSP0230, *WS-CIM Mapping Specification 1.0*,
20 http://www.dmtf.org/standards/published_documents/DSP0230_1.0.pdf
- 21 DMTF DSP1009, *Sensors Profile 1.0*,
22 http://www.dmtf.org/standards/published_documents/DSP1009_1.0.pdf
- 23 DMTF DSP1011, *Physical Asset Profile 1.0*,
24 http://www.dmtf.org/standards/published_documents/DSP1011_1.0.pdf
- 25 DMTF DSP1012, *Boot Control Profile 1.0*,
26 http://www.dmtf.org/standards/published_documents/DSP1012_1.0.pdf
- 27 DMTF DSP1013, *Fan Profile 1.0*,
28 http://www.dmtf.org/standards/published_documents/DSP1013_1.0.pdf
- 29 DMTF DSP1014, *Ethernet Port Profile, 1.0*,
30 http://www.dmtf.org/standards/published_documents/DSP1014_1.0.pdf
- 31 DMTF DSP1015, *Power Supply Profile 1.0*,
32 http://www.dmtf.org/standards/published_documents/DSP1015_1.0.pdf
- 33 DMTF DSP1022, *CPU Profile 1.0*,
34 http://www.dmtf.org/standards/published_documents/DSP1022_1.0.pdf
- 35 DMTF DSP1023, *Software Inventory Profile 1.0*,
36 http://www.dmtf.org/standards/published_documents/DSP1023_1.0.pdf

- 37 DMTF DSP1024, *Text Console Redirection Profile 1.0*,
38 http://www.dmtf.org/standards/published_documents/DSP1024_1.0.pdf
- 39 DMTF DSP1025, *Software Update Profile 1.0*,
40 http://www.dmtf.org/standards/published_documents/DSP1025_1.0.pdf
- 41 DMTF DSP1026, *System Memory Profile 1.0*,
42 http://www.dmtf.org/standards/published_documents/DSP1026_1.0.pdf
- 43 DMTF DSP1027, *Power State Management Profile 1.0*,
44 http://www.dmtf.org/standards/published_documents/DSP1027_1.0.pdf
- 45 DMTF DSP1029, *OS Status Profile 1.0*,
46 http://www.dmtf.org/standards/published_documents/DSP1029_1.0.pdf
- 47 DMTF DSP1030, *Battery Profile 1.0*,
48 http://www.dmtf.org/standards/published_documents/DSP1030_1.0.pdf
- 49 DMTF DSP1033, *Profile Registration Profile 1.0*,
50 http://www.dmtf.org/standards/published_documents/DSP1033_1.0.pdf
- 51 DMTF DSP1034, *Simple Identity Management Profile 1.0*,
52 http://www.dmtf.org/standards/published_documents/DSP1034_1.0.pdf
- 53 DMTF DSP1035, *Host LAN Network Port Profile 1.0*,
54 http://www.dmtf.org/standards/published_documents/DSP1035_1.0.pdf
- 55 DMTF DSP1036, *IP Interface Profile 1.0*,
56 http://www.dmtf.org/standards/published_documents/DSP1036_1.0.pdf
- 57 DMTF DSP1037, *DHCP Client Profile 1.0*,
58 http://www.dmtf.org/standards/published_documents/DSP1037_1.0.pdf
- 59 DMTF DSP1038, *DNS Client Profile 1.0*,
60 http://www.dmtf.org/standards/published_documents/DSP1038_1.0.pdf
- 61 DMTF DSP1039, *Role Based Authorization Profile 1.0*,
62 http://www.dmtf.org/standards/published_documents/DSP1039_1.0.pdf
- 63 DMTF DSP1054, *Indications Profile 1.0*,
64 http://www.dmtf.org/standards/published_documents/DSP1054_1.0.pdf
- 65 DMTF DSP1058, *Base Desktop and Mobile Profile 1.0*,
66 http://www.dmtf.org/standards/published_documents/DSP1058_1.0.pdf
- 67 DMTF DSP1061, *BIOS Management Profile 1.0*,
68 http://www.dmtf.org/standards/published_documents/DSP1061_1.0.pdf
- 69 DMTF DSP1070, *Opaque Management Data Profile 1.0*,
70 http://www.dmtf.org/standards/published_documents/DSP1070_1.0.pdf
- 71 DMTF DSP1076, *KVM Redirection 1.0*,
72 http://www.dmtf.org/standards/published_documents/DSP1076_1.0.pdf
- 73 DMTF DSP1077, *USB Redirection Profile 1.0*,
74 http://www.dmtf.org/standards/published_documents/DSP1077_1.0.pdf
- 75 DMTF DSP1086, *Media Redirection Profile 1.0*,
76 http://www.dmtf.org/standards/published_documents/DSP1086_1.0.pdf
- 77 DMTF DSP8007 *Platform Message Registry 1.0*,
78 http://schemas.dmtf.org/wbem/messageregistry/1/dsp8007_1.0.xml

79 DMTF DSP8030, DASH Namespace Schema 1.0, <http://schemas.dmtf.org/wbem/dash/1/dash.xsd>

80 IETF RFC 2246, T. Dierks et al., *The TLS Protocol Version 1.0*, <http://www.ietf.org/rfc/rfc2246.txt>

81 IETF RFC 4106, J. Viega and D. McGrew, *The Use of Galois/Counter Mode (GCM) in IPsec*
82 *Encapsulating Security Payload (ESP)*, <http://www.rfc-editor.org/rfc/rfc4106.txt>

83 IETF RFC 4301, S. Kent, *Security Architecture for the Internet Protocol*,
84 <http://www.rfc-editor.org/rfc/rfc4301.txt>

85 IETF RFC 4303, S. Kent, *IP Encapsulating Security Payload*, <http://www.ietf.org/rfc/rfc4303.txt>

86 **2.2 Other References**

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

89 **3 Terms and Definitions**

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

91 **3.1**

92 **can**

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

94 **3.2**

95 **cannot**

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

97 **3.3**

98 **conditional**

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

101 **3.4**

102 **mandatory**

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

105 **3.5**

106 **may**

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

108 **3.6**

109 **need not**

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

111 **3.7**

112 **optional**

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

114 **3.8**

115 **shall**

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

- 118 **3.9**
119 **shall not**
120 indicates requirements to be followed in order to conform to the document and from which no deviation is
121 permitted
- 122 **3.10**
123 **should**
124 indicates that among several possibilities, one is recommended as particularly suitable, without
125 mentioning or excluding others, or that a certain course of action is preferred but not necessarily required
- 126 **3.11**
127 **should not**
128 indicates that a certain possibility or course of action is deprecated but not prohibited

129 **4 Symbols and Abbreviated Terms**

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

- 131 **4.1**
132 **ASF**
133 Alert Standard Format
- 134 **4.2**
135 **IANA**
136 Internet Assigned Numbers Authority
- 137 **4.3**
138 **IP**
139 Internet Protocol
- 140 **4.4**
141 **MAC**
142 Media Access Control
- 143 **4.5**
144 **MAP**
145 Management Access Point
- 146 **4.6**
147 **RMCP**
148 Remote Management and Control Protocol
- 149 **4.7**
150 **TCP**
151 Transmission Control Protocol
- 152 **4.8**
153 **TLS**
154 Transport Layer Security
- 155 **4.9**
156 **UDP**
157 User Datagram Protocol

158 **4.10**
 159 **URI**
 160 Uniform Resource Identifier

161 **4.11**
 162 **WS**
 163 Web Services

164 **5 Mandatory Profiles and Specifications**

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

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

Name	Number	Version	Description
<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	

168 **6 Optional Profiles**

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

171

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>IP Interface Profile</i>	DSP1036	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>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>Software Update Profile</i>	DSP1025	1.0	
<i>System Memory Profile</i>	DSP1026	1.0	
<i>Text Console Redirection Profile</i>	DSP1024	1.0	
<i>USB Redirection Profile</i>	DSP1077	1.0	

172 7 Protocol Implementation Requirements

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

176 7.1 Management Protocol

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

180 7.1.1 XML Namespaces

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

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

183 7.1.2 WS-Transfer

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

186

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.

187 **7.1.3 WS-Enumeration**

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

191 **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.

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

195 **7.1.3.1 WS-Enumeration Filter Dialects**

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

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

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

203 **7.1.4 WS-Eventing**

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

208 **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.

209 **7.1.4.1 WS-Eventing Messaging Security**

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

211 **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

212 7.1.4.2 WS-Eventing Delivery Mode

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

216 7.1.4.3 Subscription related property definition guidance

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

219 The value for the FailureTriggerTimeInterval property on the CIM_IndicationSubscription or
220 CIM_FilterCollectionSubscription instance created internally in response to wse:Subscribe should be to
221 30 seconds.

222 7.2 Transport Protocol

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

226 8 Security Implementation Requirements

227 This section describes transport requirements, roles and authorization, user account management, and
228 authentication.

229 8.1 Transport Requirements

230 DASH defines two security classes for HTTP 1.1 transport:

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

235 • **String = "HTTP_DIGEST"**

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

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

240 • **String = "HTTP_TLS_1"**

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

242 • **String = "HTTP_TLS_2"**

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

244 • **String = "HTTP_IPSEC"**

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

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

248 Refer to 7.1.4.1 for WS-Eventing security requirements.

249 **8.1.1 Cryptographic Algorithms and Cipher Suites**

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

252 **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 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"	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

253 **8.2 Roles and Authorization**

254 Table 8 outlines the Operational Roles supported by DASH implementations and the respective DASH
 255 requirements.

256 **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	

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

260 **8.3 User Account Management**

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

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

266

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

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

270 8.4 Authentication Mechanisms

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

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

275

Table 10 – Authentication Mechanisms

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

276 9 Discovery Requirements

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

280 9.1 Network Endpoint Discovery Stage

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

284 9.2 Management Access Point Discovery Stage

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

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

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

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

289 9.2.1 RMCP Presence Ping/Pong

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

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

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

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

299 9.2.2 WS-Management Identify Method

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

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

```

305 <s:Body>
306   <wsmid:IdentifyResponse>
307     <wsmid:ProtocolVersion> xs:anyURI </wsmid:ProtocolVersion>
308     <wsmid:ProductVendor> xs:string </wsmid:ProductVendor>
309     <wsmid:ProductVersion> xs:string </wsmid:ProductVersion>
310     <dash:DASHVersion> xs:string </dash:DASHVersion>
311     <wsmid:SecurityProfiles>
312       <wsmid:SecurityProfileName> xs:string or URI </wsmid:SecurityProfileName> +
313     </wsmid:SecurityProfiles>
314   </wsmid:IdentifyResponse>
315 </s:Body>

```

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

317

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”.
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

318 9.2.3 wsmid:Identify Security Implementation Requirements

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

321 If an implementation supports wsmid:Identify without authentication, it should support it through a URL
322 that contains the suffix “/wsman-anon/identify.”

323 9.3 Enumeration of Management Capabilities Stage

324 The DMTF *Error! Reference source not found.* *Profile Registration Profile* ([DSP1033](#)) specifies methods
325 for enumerating the management capabilities of a CIM-based management access point in a scalable
326 manner. Scalability here refers to the fact that each registered profile concisely describes support for a
327 set of related management capabilities that is independent of the number of CIM instances supported by
328 the management access point.

329 10 In-Band and Out-of-Band Traffic Requirements

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

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

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

- 337 • Sideband: TCP ports for WS-Management Service
 - 338 – OOB-WS-HTTP
 - 339 – TCP 623
 - 340 – OOB-WS-HTTPS
 - 341 – TCP 664 (If class B is implemented)
- 342 • In-band: TCP ports for WS-Management Service may be supported on the following transport
343 ports and shall be transport specific:
 - 344 – HTTP
 - 345 – HTTPS (If class B is implemented)

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

347
348
349
350
351

ANNEX A (informative)

Change Log

Version	Date	Author	Description
1.0.0a	4/3/2007	J. Kozlowski	Release as preliminary standard.
1.0.0b	8/20/2007	J. Kozlowski	Release as preliminary refresh.
1.1.0a	11/12/2007	H. Shah	Release as preliminary standard.
1.1.0	4/17/2009	Hemal Shah	1.1.0 Draft Standard.
1.1.0	6/22/2009		DMTF Standard Release

352

Bibliography

353

354 DMTF DSP2014, *Systems Management Architecture for Mobile and Desktop Hardware White Paper*
355 *1.1.0*, http://www.dmtf.org/standards/published_documents/DSP2014_1.1.0.pdf
356 (Informative text in this document details Protocol, Security, and Discovery.)

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

359