DASH Implementation Requirements

Supersedes: 1.1.0
Document Type: Specification
Document Class: Normative
Document Status: Published
Document Language: en-US
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patent owner or claimant, and shall have no liability or responsibility for costs or losses incurred if a standard is withdrawn or modified after publication, and shall be indemnified and held harmless by any party implementing the standard from any and all claims of infringement by a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

36 Foreword .............................................................................................................................................. 5
37 Introduction ......................................................................................................................................... 6
38 1 Scope ............................................................................................................................................... 7
39 2 Normative references .................................................................................................................... 7
40 2.1 Approved references .................................................................................................................... 7
41 2.2 Other references ........................................................................................................................ 9
42 3 Terms and definitions ...................................................................................................................... 10
43 4 Symbols and abbreviated terms ...................................................................................................... 11
44 5 Mandatory profiles and specifications .......................................................................................... 12
45 6 Optional profiles ............................................................................................................................ 13
46 7 Protocol implementation requirements ......................................................................................... 14
47 7.1 Management protocol ................................................................................................................. 14
48 7.2 Transport protocol ....................................................................................................................... 17
49 8 Security implementation requirements ......................................................................................... 17
50 8.1 Transport requirements ............................................................................................................... 17
51 8.2 Roles and authorization ............................................................................................................ 18
52 8.3 User account management ......................................................................................................... 19
53 8.4 Authentication mechanisms ....................................................................................................... 20
54 9 Discovery requirements .................................................................................................................. 20
55 9.1 Network endpoint discovery stage ............................................................................................ 20
56 9.2 Management Access Point (MAP) discovery stage .................................................................... 20
57 9.3 Enumeration of management capabilities stage ......................................................................... 22
58 9.4 RegisteredSpecification instance .............................................................................................. 22
59 10 In-band and out-of-band traffic requirements .............................................................................. 23
60 ANNEX A (informative) Change log ............................................................................................... 24
61 Bibliography ...................................................................................................................................... 25

63 Tables

64 Table 1 – Mandatory profiles and specifications ............................................................................. 12
65 Table 2 – Optional profiles ................................................................................................................. 13
66 Table 3 – WS-Transfer operations ..................................................................................................... 14
67 Table 4 – WS-Enumeration operations ........................................................................................ ..... 15
68 Table 5 – WS-Eventing operations ................................................................................................... 16
69 Table 6 – WS-Eventing message security recommendations ............................................................ 16
70 Table 7 – Required cryptographic algorithms or cipher suites ......................................................... 18
71 Table 8 – Operational roles supported by DASH ............................................................................... 18
72 Table 9 – User account operations ................................................................................................... 19
73 Table 10 – Authentication mechanisms ............................................................................................. 20
74 Table 11 – WS-Management IdentifyResponse payload elements ................................................... 21
75 Table 12 – CIM_RegisteredSpecification element requirements ..................................................... 23
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 Company
- Jeff Hilland – Hewlett-Packard Company
- 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 1.2.
DASH Implementation Requirements

1 Scope

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

2 Normative references

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

2.1 Approved references

DMTF DSP0136, Alert Standard Format Specification 2.0,

DMTF DSP0200, CIM Operations over HTTP 1.3,
http://www.dmtf.org/standards/published_documents/DSP0200_1.3.pdf

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

DMTF DSP0227, WS-Management CIM Binding Specification 1.0,
http://www.dmtf.org/standards/published_documents/DSP0227_1.0.pdf

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

DMTF DSP1009, Sensors Profile 1.0,
http://www.dmtf.org/standards/published_documents/DSP1009_1.0.pdf

DMTF DSP1009, Sensors Profile, 1.1,

DMTF DSP1010, Record Log Profile, 2.0,

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

DMTF DSP1012, Boot Control Profile 1.0,
http://www.dmtf.org/standards/published_documents/DSP1012_1.0.pdf

DMTF DSP1013, Fan Profile 1.0,
http://www.dmtf.org/standards/published_documents/DSP1013_1.0.pdf

DMTF DSP1014, Ethernet Port Profile, 1.0,
http://www.dmtf.org/standards/published_documents/DSP1014_1.0.pdf
DMTF DSP1015, Power Supply Profile 1.0,
http://www.dmtf.org/standards/published_documents/DSP1015_1.0.pdf

DMTF DSP1015, Power Supply Profile, 1.1,

DMTF DSP1016, Telnet Service Profile, 1.0,
http://www.dmtf.org/standards/published_documents/DSP1016_1.0.pdf

DMTF DSP1017, SSH Service Profile, 1.0,
http://www.dmtf.org/standards/published_documents/DSP1017_1.0.pdf

DMTF DSP1018, Service Processor Profile, 1.1,

DMTF DSP1022, CPU Profile 1.0,
http://www.dmtf.org/standards/published_documents/DSP1022_1.0.pdf

DMTF DSP1023, Software Inventory Profile 1.0,
http://www.dmtf.org/standards/published_documents/DSP1023_1.0.pdf

DMTF DSP1024, Text Console Redirection Profile 1.0,
http://www.dmtf.org/standards/published_documents/DSP1024_1.0.pdf

DMTF DSP1025, Software Update Profile 1.0,
http://www.dmtf.org/standards/published_documents/DSP1025_1.0.pdf

DMTF DSP1026, System Memory Profile 1.0,
http://www.dmtf.org/standards/published_documents/DSP1026_1.0.pdf

DMTF DSP1027, Power State Management Profile 1.0,
http://www.dmtf.org/standards/published_documents/DSP1027_1.0.pdf

DMTF DSP1029, OS Status Profile 1.0,
http://www.dmtf.org/standards/published_documents/DSP1029_1.0.pdf

DMTF DSP1029, OS Status Profile, 1.1,

DMTF DSP1030, Battery Profile 1.0,
http://www.dmtf.org/standards/published_documents/DSP1030_1.0.pdf

DMTF DSP1033, Profile Registration Profile 1.0,
http://www.dmtf.org/standards/published_documents/DSP1033_1.0.pdf

DMTF DSP1034, Simple Identity Management Profile 1.0,
http://www.dmtf.org/standards/published_documents/DSP1034_1.0.pdf

DMTF DSP1035, Host LAN Network Port Profile 1.0,
http://www.dmtf.org/standards/published_documents/DSP1035_1.0.pdf

DMTF DSP1036, IP Interface Profile 1.0,
http://www.dmtf.org/standards/published_documents/DSP1036_1.0.pdf

DMTF DSP1037, DHCP Client Profile 1.0,
http://www.dmtf.org/standards/published_documents/DSP1037_1.0.pdf

DMTF DSP1038, DNS Client Profile 1.0,
http://www.dmtf.org/standards/published_documents/DSP1038_1.0.pdf

DMTF DSP1039, Role Based Authorization Profile 1.0,
http://www.dmtf.org/standards/published_documents/DSP1039_1.0.pdf
2.2 Other references

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

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

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

3.2 cannot
used for statements of possibility and capability, whether material, physical, or causal

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

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

3.5 may
indicates a course of action permissible within the limits of the document

3.6 need not
indicates a course of action permissible within the limits of the document

3.7 optional
indicates a course of action permissible within the limits of the document

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

3.9 shall not
indicates requirements to be followed in order to conform to the document and from which no deviation is permitted

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

3.11 should not
indicates that a certain possibility or course of action is deprecated but not prohibited
4 Symbols and abbreviated terms

The following symbols and abbreviations are used in this document.

4.1 ASF
Alert Standard Format

4.2 IANA
Internet Assigned Numbers Authority

4.3 IP
Internet Protocol

4.4 MAC
Media Access Control

4.5 MAP
Management Access Point

4.6 RMCP
Remote Management and Control Protocol

4.7 TCP
Transmission Control Protocol

4.8 TLS
Transport Layer Security

4.9 UDP
User Datagram Protocol

4.10 URI
Uniform Resource Identifier

4.11 WS
Web Services
5 Mandatory profiles and specifications

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Number</th>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Desktop and Mobile Profile</td>
<td>DSP1058</td>
<td>1.0</td>
<td></td>
</tr>
<tr>
<td>Profile Registration Profile</td>
<td>DSP1033</td>
<td>1.0</td>
<td></td>
</tr>
<tr>
<td>Role Based Authorization Profile</td>
<td>DSP1039</td>
<td>1.0</td>
<td></td>
</tr>
<tr>
<td>Simple Identity Management Profile</td>
<td>DSP1034</td>
<td>1.0</td>
<td></td>
</tr>
<tr>
<td>WS-Management Specification</td>
<td>DSP0226</td>
<td>1.0</td>
<td></td>
</tr>
<tr>
<td>WS-Management CIM Binding Specification</td>
<td>DSP0227</td>
<td>1.0</td>
<td></td>
</tr>
<tr>
<td>WS-CIM Mapping Specification</td>
<td>DSP0230</td>
<td>1.0</td>
<td></td>
</tr>
</tbody>
</table>
6 Optional profiles

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

Table 2 – Optional profiles

<table>
<thead>
<tr>
<th>Name</th>
<th>Number</th>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Battery Profile</td>
<td>DSP1030</td>
<td>1.0</td>
<td></td>
</tr>
<tr>
<td>BIOS Management Profile</td>
<td>DSP1061</td>
<td>1.0</td>
<td></td>
</tr>
<tr>
<td>Boot Control Profile</td>
<td>DSP1012</td>
<td>1.0</td>
<td></td>
</tr>
<tr>
<td>CPU Profile</td>
<td>DSP1022</td>
<td>1.0</td>
<td></td>
</tr>
<tr>
<td>DHCP Client Profile</td>
<td>DSP1037</td>
<td>1.0</td>
<td></td>
</tr>
<tr>
<td>DNS Client Profile</td>
<td>DSP1038</td>
<td>1.0</td>
<td></td>
</tr>
<tr>
<td>Ethernet Port Profile</td>
<td>DSP1014</td>
<td>1.0</td>
<td></td>
</tr>
<tr>
<td>Fan Profile</td>
<td>DSP1013</td>
<td>1.0</td>
<td></td>
</tr>
<tr>
<td>Host LAN Network Port Profile</td>
<td>DSP1035</td>
<td>1.0</td>
<td></td>
</tr>
<tr>
<td>Indications Profile</td>
<td>DSP1054</td>
<td>1.0</td>
<td>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 Platform Message Registry (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.</td>
</tr>
<tr>
<td>Indicator LED Profile</td>
<td>DSP1074</td>
<td>1.0</td>
<td></td>
</tr>
<tr>
<td>IP Interface Profile</td>
<td>DSP1036</td>
<td>1.0</td>
<td></td>
</tr>
<tr>
<td>IP Configuration Profile</td>
<td>DSP1116</td>
<td>1.0</td>
<td></td>
</tr>
<tr>
<td>KVM Redirection Profile</td>
<td>DSP1076</td>
<td>1.0</td>
<td></td>
</tr>
<tr>
<td>Media Redirection Profile</td>
<td>DSP1086</td>
<td>1.0</td>
<td></td>
</tr>
<tr>
<td>Opaque Management Data Profile</td>
<td>DSP1070</td>
<td>1.0</td>
<td></td>
</tr>
<tr>
<td>OS Status Profile</td>
<td>DSP1029</td>
<td>1.0</td>
<td></td>
</tr>
<tr>
<td>OS Status Profile</td>
<td>DSP1029</td>
<td>1.1</td>
<td></td>
</tr>
<tr>
<td>PCI Device Profile</td>
<td>DSP1075</td>
<td>1.0</td>
<td></td>
</tr>
<tr>
<td>Physical Asset Profile</td>
<td>DSP1011</td>
<td>1.0</td>
<td></td>
</tr>
<tr>
<td>Physical Computer System View Profile</td>
<td>DSP1108</td>
<td>1.0</td>
<td></td>
</tr>
<tr>
<td>Power State Management Profile</td>
<td>DSP1027</td>
<td>1.0</td>
<td></td>
</tr>
<tr>
<td>Power State Management Profile</td>
<td>DSP1027</td>
<td>2.0</td>
<td></td>
</tr>
<tr>
<td>Power Supply Profile</td>
<td>DSP1015</td>
<td>1.0</td>
<td></td>
</tr>
<tr>
<td>Power Supply Profile</td>
<td>DSP1015</td>
<td>1.1</td>
<td></td>
</tr>
<tr>
<td>Record Log Profile</td>
<td>DSP1010</td>
<td>2.0</td>
<td></td>
</tr>
<tr>
<td>Sensors Profile</td>
<td>DSP1009</td>
<td>1.0</td>
<td></td>
</tr>
</tbody>
</table>
7 Protocol implementation requirements

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

7.1 Management protocol

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

7.1.1 XML namespaces

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

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

7.1.2 WS-Transfer

It is mandatory for DASH implementations to support WS-Transfer as described in clause 7 of DSP0226. Table 3 defines support for WS-Transfer operations and their respective DASH requirements.

<table>
<thead>
<tr>
<th>Operation</th>
<th>Requirement</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Get</td>
<td>Mandatory</td>
<td>This operation retrieves resource representations.</td>
</tr>
<tr>
<td>Put</td>
<td>Conditional</td>
<td>This operation updates resources. If an implemented profile requires ModifyInstance support, the Put operation shall be supported to fulfill that requirement.</td>
</tr>
<tr>
<td>Create</td>
<td>Conditional</td>
<td>This operation creates resource instances. If an implemented profile requires CreateInstance support, the Create operation shall be supported.</td>
</tr>
<tr>
<td>Delete</td>
<td>Conditional</td>
<td>This operation deletes resources. If an implemented profile requires DeleteInstance support, the Delete operation shall be supported.</td>
</tr>
</tbody>
</table>
7.1.3 WS-Enumeration

It is mandatory for DASH implementations to support WS-Enumeration as described in clause 8 of DSP0226. Table 4 defines support for WS-Enumeration operations and their respective DASH requirements.

<table>
<thead>
<tr>
<th>Operation</th>
<th>Requirement</th>
<th>Messages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enumerate</td>
<td>Mandatory</td>
<td>This operation is used to initiate an enumeration and receive an enumeration context.</td>
</tr>
<tr>
<td>Pull</td>
<td>Mandatory</td>
<td>This operation is used to pull a sequence of elements of a resource.</td>
</tr>
<tr>
<td>Renew</td>
<td>Optional</td>
<td>See Rule R8.1-4 in DSP0226. Implementation of this operation is not recommended.</td>
</tr>
<tr>
<td>GetStatus</td>
<td>Optional</td>
<td>See Rule R8.1-4 in DSP0226. Implementation of this operation is not recommended.</td>
</tr>
<tr>
<td>Release</td>
<td>Mandatory</td>
<td>This operation is used to release an enumeration context.</td>
</tr>
<tr>
<td>EnumerationEnd</td>
<td>Optional</td>
<td>See Rule R8.1-4 in DSP0226. Implementation of this operation is not recommended.</td>
</tr>
</tbody>
</table>

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

7.1.3.1 WS-Enumeration Filter Dialects

It is optional for DASH implementations to support Selector Filter Dialect for filtered enumeration and subscription as described in ANNEX E of DSP0226. This recommendation does not contravene Rule R8.2.1-5 of DSP0226.

It is optional for DASH implementations to support Association Queries with the dialect filter URI as specified in DSP0227.

It is optional for DASH implementations to support the CQL filter dialect for enumeration as described in clause 7.1 of DSP0227. This clause does not contravene Rule R8.2.1-5 of DSP0226.
7.1.4 WS-Eventing

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

Table 5 – WS-Eventing operations

<table>
<thead>
<tr>
<th>Operation</th>
<th>Requirement</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subscribe</td>
<td>Mandatory</td>
<td></td>
</tr>
<tr>
<td>Renew</td>
<td>Mandatory</td>
<td></td>
</tr>
<tr>
<td>Unsubscribe</td>
<td>Mandatory</td>
<td></td>
</tr>
<tr>
<td>SubscriptionEnd</td>
<td>Optional</td>
<td></td>
</tr>
<tr>
<td>GetStatus</td>
<td>Optional</td>
<td>See Rule R10.3-1 in DSP0226. Implementation of this operation is not recommended.</td>
</tr>
</tbody>
</table>

7.1.4.1 WS-Eventing messaging security

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

Table 6 – WS-Eventing message security recommendations

<table>
<thead>
<tr>
<th>Plane</th>
<th>WS-Eventing Message</th>
<th>Recommended Security Class</th>
<th>Security Principal Requiring Authentication</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control</td>
<td>wse:Subscribe</td>
<td>Class B as defined in clause 8.1, because it can carry sensitive information</td>
<td>Subscriber</td>
</tr>
<tr>
<td></td>
<td>wse:Renew</td>
<td>Class B, because it can carry sensitive information</td>
<td>Subscriber</td>
</tr>
<tr>
<td></td>
<td>wse:SubscriptionEnd</td>
<td>Class B, because it can carry sensitive information</td>
<td>Subscriber</td>
</tr>
<tr>
<td></td>
<td>wse:Unsubscribe</td>
<td>Class B, because it can carry sensitive information</td>
<td>Subscriber</td>
</tr>
<tr>
<td>Delivery</td>
<td>wse:Delivery (Push)</td>
<td>Class A or B as defined in clause 8.1 (B for sensitive information or for more compute-intensive information)</td>
<td>MAP, but not necessarily with its own credentials</td>
</tr>
<tr>
<td></td>
<td>wse:Delivery (PushWithAck)</td>
<td>Class A or B (B for sensitive information)</td>
<td>MAP, but not necessarily with its own credentials</td>
</tr>
<tr>
<td></td>
<td>wse:Delivery (Batched)</td>
<td>Class A or B (B for sensitive information)</td>
<td>MAP, but not necessarily with its own credentials</td>
</tr>
<tr>
<td></td>
<td>wsen:Pull (Pull delivery)</td>
<td>Class A or B (B for sensitive information)</td>
<td>Subscriber</td>
</tr>
</tbody>
</table>
7.1.4.2 WS-Eventing delivery mode

DASH implementations shall support WS-Eventing Push Mode as described in clause 10.2.9.2 of DSP0226. DASH implementations should support WS-Eventing PushWithAck Mode as described in clause 10.2.9.3 of DSP0226.

7.1.4.3 Subscription related property definition guidance

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

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

7.2 Transport protocol

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

8 Security implementation requirements

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

8.1 Transport requirements

DASH defines two security classes for HTTP 1.1 transport:

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

   - String = "HTTP_DIGEST"
   - URI = http://schemas.dmtf.org/wbem/wsman/1/wsman/secprofile/http/digest

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

   - String = "HTTP_TLS_1"
   - URI = http://schemas.dmtf.org/wbem/wsman/1/wsman/secprofile/https/digest

   - String = "HTTP_TLS_2"
   - URI = http://schemas.dmtf.org/wbem/wsman/1/wsman/secprofile/https/basic

   - String = "HTTP_IPSEC"
   - URI = http://schemas.dmtf.org/wbem/wsman/1/wsman/secprofile/http/digest/ipsec

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

Refer to 7.1.4.1 for WS-Eventing security requirements.
### 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 section.

<table>
<thead>
<tr>
<th>Security Profile</th>
<th>Required Algorithm(s) or Cipher suite</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;HTTP_DIGEST&quot;</td>
<td>MD5</td>
<td></td>
</tr>
<tr>
<td>&quot;HTTP_TLS_1&quot;</td>
<td>TLS_RSA_WITH_AES_128_CBC_SHA (for TLS) and MD5 (for HTTP digest)</td>
<td>TLS version 1.0 or later Refer to RFC 2246, RFC 4346, RFC 5246 and RFC 3268. It is recommended that the latest 1.x version of TLS is implemented.</td>
</tr>
<tr>
<td>&quot;HTTP_TLS_2&quot;</td>
<td>TLS_RSA_WITH_AES_128_CBC_SHA</td>
<td>TLS version 1.0 or later Refer to RFC 2246, RFC 4346, RFC 5246 and RFC 3268. It is recommended that the latest 1.x version of TLS is implemented.</td>
</tr>
<tr>
<td>&quot;HTTP_IPSEC&quot;</td>
<td>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</td>
<td>Refer to RFC 4301, 4303, and 4106</td>
</tr>
</tbody>
</table>

### 8.2 Roles and authorization

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

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

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

---

18 Published Version 1.2.0
8.3 User account management

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

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

<table>
<thead>
<tr>
<th>Operation</th>
<th>Requirement</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create an account</td>
<td>Optional</td>
<td>Recommended for the administrator role</td>
</tr>
<tr>
<td>Delete an account</td>
<td>Optional</td>
<td>Recommended for the administrator role</td>
</tr>
<tr>
<td>Enable an account</td>
<td>Optional</td>
<td></td>
</tr>
<tr>
<td>Disable an account</td>
<td>Optional</td>
<td></td>
</tr>
<tr>
<td>Modify the privileges of an account</td>
<td>Optional</td>
<td></td>
</tr>
<tr>
<td>Modify the password of an account</td>
<td>Mandatory</td>
<td>Required for the administrator account.</td>
</tr>
<tr>
<td>Change the role of an account</td>
<td>Optional</td>
<td></td>
</tr>
<tr>
<td>Create a group of accounts</td>
<td>Optional</td>
<td></td>
</tr>
<tr>
<td>Delete a group of accounts</td>
<td>Optional</td>
<td></td>
</tr>
<tr>
<td>Add an account to a group</td>
<td>Optional</td>
<td></td>
</tr>
<tr>
<td>Remove an account from a group</td>
<td>Optional</td>
<td></td>
</tr>
<tr>
<td>Change the role of a group</td>
<td>Optional</td>
<td></td>
</tr>
<tr>
<td>Modify the privileges of a group</td>
<td>Optional</td>
<td></td>
</tr>
<tr>
<td>Change the associations of roles and accounts</td>
<td>Optional</td>
<td>Recommended for the administrator role</td>
</tr>
</tbody>
</table>

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

All operations defined in Table 9 shall be performed using operations as defined in DMTF DSP1039, Role Based Authorization Profile, 1.0 and DMTF DSP1034, Simple Identity Management Profile, 1.0.
8.4 Authentication mechanisms

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

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

<table>
<thead>
<tr>
<th>Authentication Mechanisms</th>
<th>Requirement</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Machine-Level</td>
<td>Optional</td>
<td></td>
</tr>
<tr>
<td>User-Level</td>
<td>Mandatory</td>
<td></td>
</tr>
<tr>
<td>Third-Party</td>
<td>Optional</td>
<td></td>
</tr>
</tbody>
</table>

9 Discovery requirements

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

9.1 Network endpoint discovery stage

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

9.2 Management Access Point (MAP) discovery stage

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

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

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

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

9.2.1 RMCP Presence Ping/Pong

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

The format of the RMCP Presence Pong (40h) data section shall conform to clause 3.2.4.3 of DSP0136 with the following definition:

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

A DASH-compliant MAP should support this command on the ASF-RMCP well-known UDP port (623) and/or well-known UDP port (664).
9.2.2 WS-Management Identify method

Refer to clause 11 of DSP0226 for a definition of the Identify method. A DASH-compliant management service shall support the Identify method on each TCP port on which WS-Management service is supported.

In addition to the child element defined in DSP0226, the following extension elements are defined by DASH as children of the IdentifyResponse element:

```
<s:Body>
    <wsmid:IdentifyResponse>
        <wsmid:ProductVendor> xs:string </wsmid:ProductVendor>
        <dash:DASHVersion> xs:string </dash:DASHVersion>
        <wsmid:SecurityProfiles>
            <wsmid:SecurityProfileName> xs:string or URI </wsmid:SecurityProfileName> +
        </wsmid:SecurityProfiles>
    </wsmid:IdentifyResponse>
</s:Body>
```

Table 11 defines the IdentifyResponse payload requirements for DASH 1.1.

<table>
<thead>
<tr>
<th>Element</th>
<th>Requirement</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>wsmid:IdentifyResponse</td>
<td>Mandatory</td>
<td>The body of the response</td>
</tr>
<tr>
<td>wsmid:IdentifyResponse/wsmid:ProductVendor</td>
<td>Optional</td>
<td></td>
</tr>
<tr>
<td>wsmid:IdentifyResponse/wsmid:ProductVersion</td>
<td>Optional</td>
<td></td>
</tr>
<tr>
<td>wsmid:IdentifyResponse/dash:DASHVersion</td>
<td>Mandatory</td>
<td>Identifies the version of the DASH Implementation Requirements 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”.</td>
</tr>
</tbody>
</table>
### 9.2.3 wsmid:Identify security implementation requirements

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

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

### 9.3 Enumeration of management capabilities stage

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

### 9.4 RegisteredSpecification instance

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

Table 12 identifies the element requirements for CIMRegisteredSpecification.
Table 12 – CIM_RegisteredSpecification element requirements

<table>
<thead>
<tr>
<th>Element</th>
<th>Requirement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Properties</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>InstanceID</td>
<td>Mandatory</td>
<td>Key, see schema definition.</td>
</tr>
<tr>
<td>SpecificationType</td>
<td>Mandatory</td>
<td>This property shall have a value of 3 (&quot;Initiative Wrapper &quot;).</td>
</tr>
<tr>
<td>RegisteredOrganization</td>
<td>Mandatory</td>
<td>This property shall have a value of 2 (DMTF).</td>
</tr>
<tr>
<td>RegisteredName</td>
<td>Mandatory</td>
<td>This property shall have a value of &quot;DASH&quot;.</td>
</tr>
<tr>
<td>RegisteredVersion</td>
<td>Mandatory</td>
<td>This property shall have a value of “1.2.0”.</td>
</tr>
<tr>
<td>AdvertiseTypes</td>
<td>Mandatory</td>
<td>Required, see Schema definition.</td>
</tr>
<tr>
<td>AdvertiseTypeDescriptions</td>
<td>Mandatory</td>
<td>See Schema definition.</td>
</tr>
<tr>
<td><strong>Operations</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>GetInstance</td>
<td>Mandatory</td>
<td></td>
</tr>
<tr>
<td>EnumerateInstances</td>
<td>Mandatory</td>
<td></td>
</tr>
<tr>
<td>EnumerateInstanceNames</td>
<td>Mandatory</td>
<td></td>
</tr>
</tbody>
</table>

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

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

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

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

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

- Sideband: TCP ports for WS-Management Service
  - OOB-WS-HTTP
    - TCP 623
  - OOB-WS-HTTPS
    - TCP 664 (If class B is implemented)

- In-band: TCP ports for WS-Management Service may be supported on the following transport ports and shall be transport specific:
  - HTTP
  - HTTPS (If class B is implemented)

NOTE In-band and out-of-band MAPs shall listen on different ports.
ANNEX A

(informative)

Change log

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0.0</td>
<td>2009-05-19</td>
<td></td>
</tr>
<tr>
<td>1.1.0</td>
<td>2009-06-22</td>
<td>DMTF Standard</td>
</tr>
<tr>
<td>1.2.0</td>
<td>2014-12-22</td>
<td>DMTF Standard</td>
</tr>
</tbody>
</table>
Bibliography
