Document Identifier: DSP0232

Date: 2024-01-05

Version: 1.4.0

DASH Implementation Requirements

Supersedes: 1.3.1

Document Class: Normative

Document Status: Published

Document Language: en-US

CONTENTS

Foreword 4
Introduction 5
1 Scope 6
2 Normative references 6
3 Terms and definitions 9
4 Symbols and abbreviated terms 10
5 Mandatory profiles and specifications 11
6 Optional profiles 12
7 Protocol implementation requirements 13
7.1 Management protocol 13
7.2 Transport protocol 16
8 Security implementation requirements 16
8.1 Transport requirements 16
8.2 Roles and authorization 18
8.3 User account management 18
8.4 Authentication mechanisms 19
9 Discovery requirements 19
9.1 Network endpoint discovery stage 19
9.2 Management access point discovery stage 19
9.3 Enumeration of management capabilities stage 22
9.4 RegisteredSpecification instance 22
10 In-band and out-of-band traffic requirements 22
ANNEX A (informative) Change log 24
Bibliography 25

Tables

Table 1 – Mandatory profiles and specifications 11
Table 2 – Optional profiles 12
Table 3 – WS-Transfer operations 14
Table 4 – WS-Enumeration operations 14
Table 5 – WS-Eventing operations 15
Table 6 – WS-Eventing message security recommendations 15
Table 7 – Required cryptographic algorithms or cipher suites 17
Table 8 – Operational roles supported by DASH 18
Table 9 – User account operations 18
Table 10 – Authentication mechanisms 19
Table 11 – WS-Management IdentifyResponse payload elements 20
Table 12 – CIM_RegisteredSpecification element requirements 22

Foreword

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

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

Acknowledgments

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

Editors:

- Hemal Shah – Broadcom Inc.
- Joe Kozlowski – Dell Inc.
- Steven Breed – Dell Inc.
- Divyanand Malavalli – Advanced Micro Devices

Contributors:

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

Introduction

This specification describes the conformance requirements for implementing the Desktop and Mobile Architecture for System Hardware (DASH) version 1.4.

1 Scope

This document describes the requirements for implementing the Desktop and Mobile Architecture for System Hardware version 1.4. 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 or versioned references, only the edition cited (including any corrigenda or DMTF update versions) applies. For references without a date or version, the latest published edition of the referenced document (including any corrigenda or DMTF update versions) applies.

DMTF DSP0004, *Common Information Model (CIM) Infrastructure 2.6,*
https://www.dmtf.org/standards/published_documents/DSP0004_2.6.pdf

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

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

DMTF DSP0223, *Generic Operations 2.0*,
https://www.dmtf.org/sites/default/files/standards/documents/DSP0223_2.0.0.pdf

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

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

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

DMTF DSP1001, *Management Profile Specification Usage Guide 1.1,*
https://www.dmtf.org/standards/published_documents/DSP1001_1.1.pdf

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

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

DMTF DSP1009, *Sensors Profile 1.2*,
https://www.dmtf.org/sites/default/files/standards/documents/DSP1009_1.2.0.pdf

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

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

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

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

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

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

DMTF DSP1015, *Power Supply Profile 1.1*,
https://www.dmtf.org/sites/default/files/standards/documents/DSP1015_1.1.pdf

DMTF DSP1016, *Telnet Service Profile 1.0*,
https://www.dmtf.org/sites/default/files/standards/documents/DSP1016_1.0.pdf

DMTF DSP1017, *SSH Service Profile 1.0*,
https://www.dmtf.org/sites/default/files/standards/documents/DSP1017_1.0.pdf

DMTF DSP1018, *Service Processor Profile 1.1*,
https://www.dmtf.org/standards/published_documents/DSP1018_1.1.pdf

DMTF DSP1022, *CPU Profile 1.0*,
https://www.dmtf.org/sites/default/files/standards/documents/DSP1022_1.0.pdf

DMTF DSP1023, *Software Inventory Profile 1.0,*
https://www.dmtf.org/sites/default/files/standards/documents/DSP1023_1.0.pdf

DMTF DSP1024, *Text Console Redirection Profile 1.0,*
https://www.dmtf.org/sites/default/files/standards/documents/DSP1024_1.0.2.pdf

DMTF DSP1025, *Software Update Profile 1.0,*
https://www.dmtf.org/sites/default/files/standards/documents/DSP1025_1.0.pdf

DMTF DSP1026, *System Memory Profile 1.0*,
https://www.dmtf.org/sites/default/files/standards/documents/DSP1026_1.0.pdf

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

DMTF DSP1027, *Power State Management Profile 2.0*,
https://www.dmtf.org/standards/published_documents/DSP1027_2.0.pdf

DMTF DSP1029, *OS Status Profile 1.0,*
https://www.dmtf.org/sites/default/files/standards/documents/DSP1029_1.0.pdf

DMTF DSP1029, *OS Status Profile 1.1*,
https://www.dmtf.org/sites/default/files/standards/documents/DSP1029_1.1.pdf

DMTF DSP1030, *Battery Profile 1.0,*
https://www.dmtf.org/sites/default/files/standards/documents/DSP1030_1.0.pdf

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

DMTF DSP1033, *Profile Registration Profile 1.1,*
https://www.dmtf.org/standards/published_documents/DSP1033_1.1.pdf

DMTF DSP1034, *Simple Identity Management Profile 1.0*,
https://www.dmtf.org/sites/default/files/standards/documents/DSP1034_1.0.pdf

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

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

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

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

DMTF DSP1039, *Role Based Authorization Profile 1.0*,
https://www.dmtf.org/standards/published_documents/DSP1039_1.0.pdf

DMTF DSP1040*, Platform Watchdog Profile 1.0*,
https://www.dmtf.org/sites/default/files/standards/documents/DSP1040_1.0.pdf

DMTF DSP1054, *Indications Profile 1.0,*
https://www.dmtf.org/sites/default/files/standards/documents/DSP1054_1.0.pdf

DMTF DSP1058, *Base Desktop and Mobile Profile 1.0*,
https://www.dmtf.org/standards/published_documents/DSP1058_1.0.pdf

DMTF DSP1061, *BIOS Management Profile 1.0,*
https://www.dmtf.org/standards/published_documents/DSP1061_1.0.pdf

DMTF DSP1070, *Opaque Management Data Profile 1.0,*
https://www.dmtf.org/standards/published_documents/DSP1070_1.0.pdf

DMTF DSP1074*, Indicator LED Profile 1.0*,
https://www.dmtf.org/standards/published_documents/DSP1074_1.0.pdf

DMTF DSP1075*, PCI Device Profile 1.0*,
https://www.dmtf.org/sites/default/files/standards/documents/DSP1075_1.0.pdf

DMTF DSP1076, *KVM Redirection Profile 1.0,*
https://www.dmtf.org/sites/default/files/standards/documents/DSP1076_1.0.pdf

DMTF DSP1077, *USB Redirection Profile 1.0,*
https://www.dmtf.org/sites/default/files/standards/documents/DSP1077_1.0.pdf

DMTF DSP1085*, Power Utilization Management Profile 1.0*,
https://www.dmtf.org/sites/default/files/standards/documents/DSP1085_1.0.0.pdf

DMTF DSP1086, *Media Redirection Profile 1.0,*
https://www.dmtf.org/standards/published_documents/DSP1086_1.0.pdf

DMTF DSP1088*, Wi-Fi Port Profile 1.0*,
https://www.dmtf.org/sites/default/files/standards/documents/DSP1088_1.0.0.pdf

DMTF DSP1108*, Physical Computer System View Profile 1.0*,
https://www.dmtf.org/standards/published_documents/DSP1108_1.0.pdf

DMTF DSP1116*, IP Configuration Profile 1.0*,
https://www.dmtf.org/standards/published_documents/DSP1116_1.0.pdf

DMTF DSP8007 *Platform Message Registry 1.0*,
http://schemas.dmtf.org/wbem/messageregistry/1/dsp8007_1.0.xml

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

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

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

IETF RFC 4301, S. Kent, *Security Architecture for the Internet Protocol*, https://www.rfc-editor.org/rfc/rfc4301.txt

IETF RFC 4303, S. Kent, *IP Encapsulating Security Payload (ESP)*, https://www.ietf.org/rfc/rfc4303.txt

IETF RFC 4346, T. Dierks et al., *The Transport Layer Security (TLS) Protocol Version 1.1*, https://www.ietf.org/rfc/rfc4346.txt

IETF RFC 5246, T. Dierks et al., *The Transport Layer Security (TLS) Protocol Version 1.2*, https://www.ietf.org/rfc/rfc5246.txt

IETF RFC 8446, E. Rescorla et al., *The Transport Layer Security (TLS) Protocol Version 1.3*, https://www.ietf.org/rfc/rfc8446.txt

ISO/IEC Directives, Part 2, *Principles and rules for the structure and drafting of ISO and IEC documents*, https://www.iso.org/sites/directives/current/part2/index.xhtml

3 Terms and definitions

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

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

The terms "clause", "subclause", "paragraph", and "annex" in this document are to be interpreted as described in ISO/IEC Directives, Part 2, Clause 6.

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

The terms defined in DSP0004, DSP0223, and DSP1001 apply to this document. The following additional terms are used in this document.

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 1 – Mandatory profiles and specifications

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

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. For an optional profile with multiple versions listed in the table below, one or more versions of the optional profile may be implemented. If implemented, the latest version of the optional profile should be implemented.

Table 2 – Optional profiles

Name	Number	Version	Description
Battery Profile	DSP1030	1.0	
BIOS Management Profile	DSP1061	1.0	
Boot Control Profile	DSP1012	1.0	
CPU Profile	DSP1022	1.0	
DHCP Client Profile	DSP1037	1.0	
DNS Client Profile	DSP1038	1.0	
Ethernet Port Profile	DSP1014	1.0	
Fan Profile	DSP1013	1.0	
Host LAN Network Port Profile	DSP1035	1.0	
Indications Profile	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 *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.
Indicator LED Profile	DSP1074	1.0	
IP Interface Profile	DSP1036	1.0	
IP Configuration Profile	DSP1116	1.0	
KVM Redirection Profile	DSP1076	1.0	
Media Redirection Profile	DSP1086	1.0	
Opaque Management Data Profile	DSP1070	1.0	
OS Status Profile	DSP1029	1.0	
OS Status Profile	DSP1029	1.1	
PCI Device Profile	DSP1075	1.0	
Physical Asset Profile	DSP1011	1.0	
Physical Computer System View Profile	DSP1108	1.0	
Power State Management Profile	DSP1027	1.0	
Power State Management Profile	DSP1027	2.0	
Power Supply Profile	DSP1015	1.0	
Power Supply Profile	DSP1015	1.1	
Profile Registration Profile	DSP1033	1.1	

Name	Number	Version	Description
Power Utilization Management Profile	DSP1085	1.0	Represent and manage power utilization configuration.
Record Log Profile	DSP1010	2.0	
Sensors Profile	DSP1009	1.0	
Sensors Profile	DSP1009	1.1	
Sensors Profile	DSP1009	1.2	
Service Processor Profile	DSP1018	1.1	
Software Inventory Profile	DSP1023	1.0	
Software Update Profile	DSP1025	1.0	
SSH Service Profile	DSP1017	1.0	
System Memory Profile	DSP1026	1.0	
Telnet Service Profile	DSP1016	1.0	
Text Console Redirection Profile	DSP1024	1.0	
USB Redirection Profile	DSP1077	1.0	
Watchdog Profile	DSP1040	1.0	
Wi-Fi Port Profile	DSP1088	1.0	Represent Wi-Fi port, associated controller and Wi-Fi interfaces.

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

```
(1)   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.

352 **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.

353 ### 7.1.3 WS-Enumeration

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

357 **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.

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

361 #### 7.1.3.1 WS-Enumeration filter dialects

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

365 It is optional for DASH implementations to support *Association Queries* with the dialect filter URI as
366 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

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.

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

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

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, one of either MD5 digest algorithm or SHA-256 digest algorithm shall be supported.
   - **String = “HTTP_DIGEST”**
   - **String = “HTTP_DIGEST_SHA256”**
2) **Class B**: This class defines five 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”**
     - TLS_RSA_WITH_AES_128_CBC_SHA (for TLS) and MD5 (for HTTP digest)
   - **String = “HTTP_TLS_2”**
     - TLS_RSA_WITH_AES_128_CBC_SHA
   - **String = “HTTP_TLS_3”**
     - TLS 1.2 (TLS_DHE_RSA_WITH_AES_128_CBC_SHA256), Digest SHA-256
   - **String = “HTTP_TLS_4”**
     TLS 1.3 or later (TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256), Digest SHA-256
     For Key Exchange: ECDHE secp256r1
     For Signature Authentication: rsa_pss_rsae_sha256
     For Symmetric Cipher (Record Layer): TLS_AES_128_GCM_SHA256

- **String = “HTTP_TLS_5”**
  - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (for TLS) and MD5 (for HTTP digest)
- **String = “HTTP_IPSEC”**

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

For class B compliance, the DASH implementation shall support at least one of the security profiles HTTP_TLS_1, HTTP_TLS_2, HTTP_TLS_3, HTTP_TLS_4, HTTP_TLS_5 or HTTP_IPSEC. For enhanced security, the implementation should support either “HTTP_TLS_3” or “HTTP_TLS_4” or “HTTP_TLS_5” security profiles.

Refer to 7.1.4.1 for WS-Eventing security requirements.

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

8.1.1 Cryptographic algorithms and cipher suites

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

NOTE: Cryptographic protocols TLS 1.0 and TLS 1.1 are deprecated.

Table 7 – Required cryptographic algorithms or cipher suites

Security Profile	Required Algorithm(s) or Cipher suite	Notes
“HTTP_DIGEST”	MD5	
“HTTP_TLS_1”	TLS_RSA_WITH_AES_128_CBC_SHA (for TLS) and MD5 (for HTTP digest)	TLS version 1.2 or later Refer to RFC 2246, RFC 4346, RFC 5246 and RFC 3268.
“HTTP_TLS_2”	TLS_RSA_WITH_AES_128_CBC_SHA	TLS version 1.2 or later Refer to RFC 2246, RFC 4346, RFC 5246 and RFC 3268.
“HTTP_TLS_3”	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 and SHA-256 (for HTTP digest)	TLS version 1.2 Refer to RFC 5246, RFC 3268 and RFC 7616
“HTTP_TLS_4”	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 and SHA-256 (for HTTP digest) For Key Exchange: ECDHE secp256r1 For Signature Authentication: rsa_pss_rsae_sha256 For Symmetric Cipher (Record Layer): TLS_AES_128_GCM_SHA256	TLS version 1.3 or later Refer to RFC 8446
“HTTP_TLS_5”	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 and MD5 (for HTTP digest)	TLS version 1.2 or later. Refer to RFC 5246 and RFC 5288

"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

8.2 Roles and authorization

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

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	

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.*

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 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	

Operation	Requirement	Notes
Change the associations of roles and accounts	Optional	Recommended for the administrator role

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 10 – Authentication mechanisms

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

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 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 clause shall conform to clause 3.2.4.3 of DSP0136 with the following definition:

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

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

479 ### 9.2.2 WS-Management identify method

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

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

```
485  <s:Body>
486    <wsmid:IdentifyResponse>
487      <wsmid:ProtocolVersion> xs:anyURI </wsmid:ProtocolVersion>
488      <wsmid:ProductVendor> xs:string </wsmid:ProductVendor>
489      <wsmid:ProductVersion> xs:string </wsmid:ProductVersion>
490      <dash:DASHVersion> xs:string </dash:DASHVersion>
491      <wsmid:SecurityProfiles>
492        <wsmid:SecurityProfileName> xs:string or URI </wsmid:SecurityProfileName> +
493      </wsmid:SecurityProfiles>
494    </wsmid:IdentifyResponse>
495  </s:Body>
```

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

497 **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 *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”.

Element	Requirement	Notes
wsmid:IdentifyResponse/wsmid:SecurityProfiles/ wsmid:SecurityProfileName	Mandatory	URI identifying the security profile supported Class A: “HTTP_DIGEST”: http://schemas.dmtf.org/wbem/wsman/1/ wsman/secprofile/http/digest "HTTP_DIGEST_SHA256": http://schemas.dmtf.org/wbem/wsman/1/ wsman/secprofile/http/digest_sha256 Class B: “HTTP_TLS_1”: http://schemas.dmtf.org/wbem/wsman/1/ wsman/secprofile/https/digest “HTTP_TLS_2”: http://schemas.dmtf.org/wbem/wsman/1/ wsman/secprofile/https/basic “HTTP_TLS_3”: http://schemas.dmtf.org/wbem/wsman/1/ wsman/secprofile/https/digest_t3 “HTTP_TLS_4”: http://schemas.dmtf.org/wbem/wsman/1/ wsman/secprofile/https/digest_t4 “HTTP_TLS_5”: http://schemas.dmtf.org/wbem/wsman/1/ wsman/secprofile/https/digest_t5 “HTTP_IPSEC”: http://schemas.dmtf.org/wbem/wsman/1/ wsman/secprofile/http/digest/ipsec

NOTE: The links in Table 11 are URIs (Uniform Resource Identifier) and defines the identity of security profile resource.

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 CIM_RegisteredSpecification to indicate support for this version of the specification.

Table 12 identifies the element requirements for CIM_RegisteredSpecification.

Table 12 – CIM_RegisteredSpecification element requirements

Element	Requirement	Description
Properties		
InstanceID	Mandatory	Key, see schema definition.
SpecificationType	Mandatory	This property shall have a value of 3 ("Initiative Wrapper ").
RegisteredOrganization	Mandatory	This property shall have a value of 2 (DMTF).
RegisteredName	Mandatory	This property shall have a value of “DASH”.
RegisteredVersion	Mandatory	This property shall have a value of “1.4.0”.
AdvertiseTypes	Mandatory	Required, see Schema definition.
AdvertiseTypeDescriptions	Mandatory	See Schema definition.
Operations		
GetInstance	Mandatory	
EnumerateInstances	Mandatory	
EnumerateInstanceNames	Mandatory	

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.

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

531 • Sideband: TCP ports for WS-Management Service
532 – OOB-WS-HTTP
533 – TCP 623
534 – OOB-WS-HTTPS
535 – TCP 664 (If class B is implemented)
536 • In-band: TCP ports for WS-Management Service may be supported on the following transport
537 ports and shall be transport specific:
538 – HTTP
539 – HTTPS (If class B is implemented)

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

ANNEX A
(informative)

Change log

Version	Date	Description
1.0.0	2009-05-19	
1.0.1	2009-10-16	Updated
1.1.0	2009-06-22	DMTF Standard Release
1.2.0	2014-12-22	DMTF Standard Release
1.2.1	2015-05-21	DMTF Standard Release
1.3.0	2021-01-08	Added TLS security enhancements.
1.3.1	2021-09-17	Reference to added Profile Registration Profile 1.1
1.4.0	2024-01-05	DMTF Standard Release 1.4. Changes: • DSP1085 and DSP1088 added under optional profiles (Section 6) • Security profile HTTP_TLS_5 added under security requirements (Section 8.1)

Bibliography

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

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